



비트코인 디플로마

비트코인을 위한 금융 교육

학습 워크북

한국어 버전 | 2025

Powered by
 Bitcoin Social Layer

My First Bitcoin has created this work and made it
freely available under [Creative Commons](#).

This work is licensed under
[Creative Commons](#)
[Attribution-ShareAlike](#)
[4.0 International \(CC BY-SA 4.0\)](#)





비트코인 디플로마

비트코인을 위한 금융 교육

학습 워크북

한국어 버전 | 2025

번역: ATOMIC BITCOIN

검수: Bitcoin Social Layer



bc1q5es60qpa7gpkp0k32x14zefkj43kd9zjkzd54sgmv3yxr34dw8dqm9pzsd

비트코인 디플로마 이야기

비트코인 시기가 도래했을 때 그것만큼 강력한 것은 없습니다.

비트코인 디플로마의 이야기는 엘살바도르에서 시작되었습니다. 2022년 6월, 첫 번째 임시 프로그램으로 38명의 공립학교 학생들이 세계 최초로 비트코인 디플로마 과정으로 졸업하였습니다.

불과 3년 전이었다는 것이 믿기지 않을 정도입니다.

그 이후로 성장세는 놀라웠습니다. 지금까지 전국 곳곳에서 수천 명의 비트코인 디플로마 졸업생이 배출되었습니다. 하지만 가장 흥미롭고 영감을 주는 성장은 학교가 아닌 곳에서 비롯되었습니다. 이 워크북은 오픈소스로 제공되며, 엘살바도르 뿐만 아니라 전 세계의 다양한 비트코인 교육자들이 이 자료를 받아들였습니다.

엘살바도르 교육부는 자체 비트코인 디플로마 주요 자료로 이 워크북을 활용했으며, 2024년에는 비트코인 비치(Bitcoin Beach)와 협력하여 400명이 넘는 공립학교 교사들에게 가르치는 수업을 진행했습니다.

우리의 원래 목표 중 하나는 한 국가를 교육시키고, 대규모 비트코인 교육이 선을 위한 힘이 될 수 있음을 입증하는 것이었습니다. 그 꿈은 이제 현실로 나아가고 있습니다.

엘살바도르는 중심이며, 우리의 사명은 전 세계로 진출 하는 것입니다.

2023년 3월, 우리는 국제 비트코인 교육자 노드 네트워크(Bitcoin Educators Node Network)를 설립했습니다. 이 네트워크에 참여하는 모든 노드는 몇 가지 핵심 원칙에 동의해야 합니다: 교육은 자유롭고 공정하며, 지역사회 주도로 진행되고, 비트코인만 다루며, 높은 품질과 역량 강화를 목표로 해야 합니다. 이 네트워크는 현재 누구의 통제 없이 운영되며, 캐나다, 미국, 멕시코, 과테말라, 온두拉斯, 코스타리카, 쿠바, 도미니카 공화국, 아이티, 콜롬비아, 수리남, 페루, 브라질, 아르헨티나, 아일랜드, 영국, 포르투갈, 조지아, 가나, 나이지리아, 우간다, 케냐, 잠비아, 짐바브웨, 남아프리카, 아프가니스탄, 방글라데시, 인도, 홍콩, 인도네시아, 호주에서 비트코인 디플로마를 가르쳤습니다. 네트워크는 매달 새로운 노드를 추가하며 오픈소스이기 때문에 누구의 허가도 필요 없습니다. 아마도 스스로 노드를 돌리는 사람들이 훨씬 더 많을 가능성이 큽니다.

이것은 전 세계를 대상으로 하는 분산화된 운동입니다.

공정하며 지역사회 주도로 이루어진 비트코인 교육은 세상을 바꿀 것입니다. 아니, 이미 세상을 바꿔가고 있습니다.

더 나은 세상을 위해,

My First Bitcoin team, 2025

목차

제 1장: 왜 우리는 돈이 필요한가?

1.0 서론	01
1.1 사토시 만나기	01
체험 활동: 돈에 대한 5가지 질문	01
1.2 수업 토론 - 왜 우리는 돈이 필요한가?	04

제 2장: 돈이란 무엇인가?

2.0 서론	07
체험 활동: 수업 토론 - 돈이란 무엇인가?	07
2.1 돈의 정의	07
2.2 돈의 기능	09
2.3 돈의 속성	10
2.4 돈의 유형	13
2.5 돈의 심리학: 희소성, 시간 선호, 트레이드-오프	14
체험 활동: 시간 선호	16

제 3장: 돈의 역사

3.0 서론	21
체험 활동: 물물교환 게임	21
3.1 물물교환에서 현대 화폐로 진화	23
3.1.1 초기 화폐 문제점	23
3.1.2 주화와 지폐의 발달	24
3.1.3 건전화폐에서 불건전화폐로 전환	25
3.1.4 지폐에서 플라스틱카드로	27
3.2 디지털 화폐	28

제 4장: 명목화폐란 무엇이며, 누가 통제하는가?

4.0 서론	31
4.1 명목화폐의 간략한 역사	31
4.2 명목화폐 시스템	34
4.2.1 법령에 의한 화폐 시스템	34

4.2.2 은행 부분지급준비 제도: 부채로 운영되는 시스템	35
체험 활동: 은행의 부분지급준비 제도	38
4.2.3 누가 명목화폐 시스템을 통제하며, 이익을 얻는 방법은 무엇인가?	39
4.3 중앙은행 디지털 화폐(CBDC): 명목화폐의 미래	41

제 5장: 문제를 어떻게 해결해야 하는가?

5.0 서론: 문제	45
5.1 구매력 감소	45
5.1.1 화폐 인플레이션과 구매력에 미치는 영향	45
체험 활동: 인플레이션 효과 - 경매	46
5.2 전 세계 부채 부담과 사회 불평등	47
5.2.1 개인에 미치는 영향 - 구매력 손실	47
5.2.2 사회에 미치는 영향 - 부의 불평등 증가	52
체험 활동: 명목화폐 시스템의 결과	53
5.2.3 전 세계의 부채 부담	54
5.3 사이퍼펑크와 분산형 화폐가 걸어온 길	55
5.3.1 사이퍼펑크	56
5.3.2 중앙화 시스템 vs 분산화 시스템	57
5.3.3 디지털 화폐의 간략한 역사	59

제 6장: 비트코인 소개

6.0 사토시 나카모토의 비트코인 창조	63
6.1 비트코인은 작동 원리는 무엇인가?	65
6.1.1 나카모토 합의 알고리즘	65
6.1.2 게임의 참여자들	67
체험 활동: 개인 대 개인 네트워크에서 합의 형성	69
6.2 디지털 건전화폐인 비트코인	71
6.2.1 서론	71
6.2.2 비트코인의 특징	72
체험 활동: 수업 토론 - 비트코인은 건전화폐인가?	76
6.2.3 책임과 권한을 이해하기	76

제 7장: 비트코인 사용법

7.0 서론	81
7.1 비트코인 획득 및 교환	81
7.1.1 P2P: 오프라인 거래	81
7.1.2 P2P: 온라인 거래	82
7.1.3 중앙화 거래소	82
7.2 비트코인 지갑 소개	83
7.2.1 셀프커스터디 지갑 vs 수탁형 지갑	83
7.2.2 비트코인 지갑의 종류	85
7.2.3 오픈 소스 vs 비공개 소스	86
체험 활동: 수업 토론 - 비트코인 지갑	87
7.3 모바일 비트코인 지갑 설정	87
체험 활동: 비트코인 지갑 설정/복구하기	87
7.4 비트코인 보내기와 받기	89
체험 활동: 실시간 비트코인 거래 체험	91
7.5 비트코인 저축	93
7.4 믿지 말고 검증하라	94

제 8장: 라이트닝 네트워크: 일상에서 비트코인 사용하기

8.0 서론	97
체험 활동: 라이트닝 네트워크 설명 영상 시청하기	98
8.1 라이트닝 네트워크	98
8.2 라이트닝 지갑 종류	100
8.2.1 셀프커스터디 지갑 vs 수탁형 지갑	100
8.2.2 오픈 소스 vs 비공개 소스	100
8.3 라이트닝 지갑 설정	100
8.4 라이트닝 보내기와 받기	102
체험 활동: 라이트닝 릴레이 레이스	106
8.5 비트코인으로 커피 마시기, 물건 구매하기	107
8.5.1 온라인: 결제 플러그인 - 전자상거래	108
8.5.2 오프라인: 주변의 결제매장 찾기	109
8.5.3 기타 전송방법: 상품권, 기프트 카드 및 직불 카드	110
8.5.4 지속 가능한 생태계와 교환 매체로서 비트코인	110

제 9장: 비트코인 기술 이해

9.0 서론	115
체험 활동: 비트코인은 작동 원리는 무엇인가? 영상시청	115
9.1 공개키와 개인키: 암호화를 통한 보안	116
9.1.1 암호화된 공개키와 개인키	116
9.1.2 해싱 설명	119
체험 활동: SHA-256 해시 생성하기	121
9.2 UTXO 모델	122
9.3 비트코인 노드와 채굴자에 대한 심층 분석	125
9.3.1 비트코인 노드란 무엇이며, 어떻게 설정하는가?	125
체험 활동: 비트코인 노드 영상 시청하기	126
9.3.2 비트코인 채굴자란 무엇이며, 어떻게 작동하는가?	126
9.4 메모리풀이란 무엇인가?	132
체험 활동: 메모리풀	134
9.5 비트코인 거래의 시작부터 완료까지의 과정	135

제 10장: 왜 비트코인인가?

10.0 서론	139
체험 활동: 비트코인은 미래는 어떤 모습일까?	139
10.1 중앙은행 디지털 화폐(CBDC)란 무엇이며, 누가 통제하는가?	140
10.2 비트코인 철학	141
체험 활동: 수업 토론 - 여러분은 돈을 통제할 권리가 있는가?	141
10.3 비트코인 이점	142
10.4 보장된 미래	143
체험 활동: 수업 토론 - 여러분의 관점은 어떻게 변했는가?	143
추가 자료	147
핵심 개념	149
용어집	153

비트코인 디플로마

자유롭고 공정하며,
좋은 품질의 무료 교육을 통해
이루어지는 10주간의 학습 여정

[비트코인](#)을 공부하기 전에 돈의 기본 개념, 역사, 그리고 현재 금융 시스템을 이해하는 것이 반드시 필요합니다. 이 개념을 이해한다면 독특하고 세상을 바꿀만한 특성을 가진 [비트코인](#)을 파악하기 위한 탄탄한 기초가 됩니다. 돈의 진화를 배우면서 현재 금융 시스템의 한계를 더 잘 이해할 수 있으며, 이것의 해결 방법은 비트코인이라는 것을 알게 될 것입니다. 이러한 기초가 없다면 비트코인의 중요성과 아직 드러나지 않은 영향을 완전히 이해하기 어려울 수 있습니다. 학습 과정을 신뢰하고 계속 집중해보세요. 이를 통해 비트코인의 깊은 이해와 지식 등의 보상이 분명 가치 있을 것입니다.

제 1장

왜 우리는 돈이 필요한가?

1.0 서론

1.1 사토시 만나기

체험 활동: 돈에 대한 5가지 질문

1.2 수업 토론 - 왜 우리는 돈이 필요한가?

학습 워크북

한국어 버전 | 2025

왜 우리는 돈이 필요한가?

1.0 서론

“

돈은 인류가 발명한 가장 위대한 자유의 도구 중 하나입니다.

프리드리히 하이에크

”

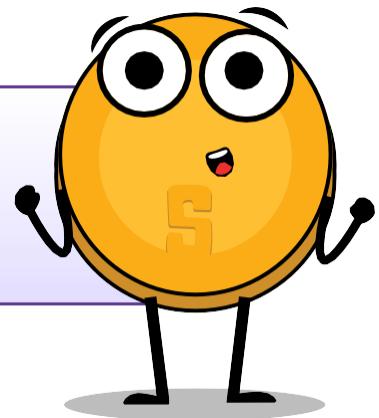
비트코인 디플로마에 오신 것을 환영합니다. 이번 장에서는 돈이 우리 삶에서 왜 중요한지, 근본 질문을 탐구해보겠습니다. 돈의 본질과 다양한 형태를 살펴보며, 그 중요성을 깊이 이해하는 데 초점을 맞출 것입니다. 우리는 거의 매일 돈을 사용하지만, 정말로 왜 돈이 필요한지, 돈이 무엇인지 이해하고 있을까요? 왜 부모님과 가족들은 시간을 돈과 바꾸는 걸까요? 왜 어떤 사람들은 더 많은 돈이 있고, 다른 사람들은 그렇지 않을까요? 왜 돈은 국가에 따라 다를까요? 필요한 만큼 돈을 그냥 만들어낼 수 없는 이유는 무엇일까요?

1.1 사토시 만나기



안녕하세요! 저는 사토시입니다.

비트코인 디플로마 과정을 도와드릴 대화형 도우미입니다.
핵심 개념을 더 깊이 이해할 수 있도록 유용한 자료를 추천하고
제공하겠습니다.



체험활동: 아래 다섯 가지 질문에 답하며 챕터를 시작해 봅시다

음식이나 원하는 물건과 같은 필수품을 얻는 실생활에서 사용되는 사례를 고려해 보세요. 예를 들어, 창의성과 현실성을 균형 있게 조화시키며 자세히 작성해 보세요.



제 1장



왜 우리는 돈이 필요한가?

돈이란 무엇인가?

왜 우리는 돈이 필요한가?

돈은 누가 통제하는가?

돈은 무엇 때문에 가치가 있는가?



제 1장

돈에 대해 궁금한 점이 무엇인가요? 여기 질문을 적어 수업 친구들과 공유 해보세요.

돈이 필요한 다섯 가지 이유를 모두에게 공유하고 비교하며 결정하세요.

수업 전체에서 가장 많이 나온 아이디어를 확인하세요.

수업 아이디어 리스트에 포함되지는 않았지만 자신만의 아이디어를 되짚어보고 적어보세요.

1.2 수업 토론 - 왜 우리는 돈이 필요한가?

수업 학생들은 그룹으로 나뉘어 다음을 진행합니다:

-  각자 네 가지 질문의 답변을 공유하고 논의하며, 가장 마음에 드는 답변을 기록합니다.
-  마지막 질문에 대한 답변을 공유하고, 가장 마음에 드는 학생의 질문을 투표로 선정한 후 그 결과를 기록합니다.
-  비트코인 디플로마 과정이 끝날 때 이 답변들과 질문들을 다시 살펴봅니다.

이제 왜 돈이 필요한지에 대해 더 명확히 이해했으니, 뒤에서는 돈이란 무엇인지, 진화한 역사, 누가 돈에 영향을 미치는지, 마지막으로 돈의 현재 형태에 대해 다룰 것입니다.

첫 수업에서 작성한 리스트를 계속 참고하며, 돈의 탄생과 정의 그리고 돈의 사용 방법이 발전한 역사를 여러분의 통찰력과 연결 지어보세요.

제 2장

돈이란 무엇인가?

2.0 서론

체험 활동: 수업 토론 - 돈이란 무엇인가?

2.1 돈의 정의

2.2 돈의 기능

2.3 돈의 속성

2.4 돈의 유형

2.5 돈의 심리학: 희소성, 시간 선호, 트레이드-오프

체험 활동: 시간 선호

학습 워크북

한국어 버전 | 2025

돈이란 무엇인가?

2.0 서론

“

돈은 우리가 미래에 원하는 것을 가질 수 있도록 보장하는 수단입니다.
지금은 필요하지 않더라도, 새로운 물건을 구매할 때 필요한 구매력을 확보해줍니다.

아리스토 텔레스

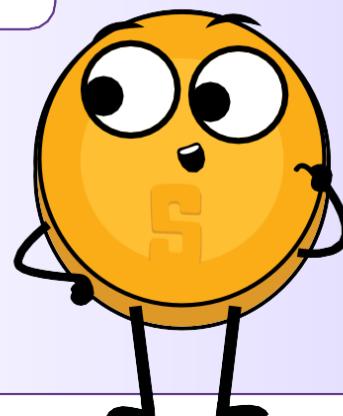
”

돈의 필요성에 대한 탐구를 바탕으로, 이번 장에서는 핵심 질문인 “돈이란 무엇인가?”를 탐구합니다. 그룹 토론과 활동으로 시작해 보겠습니다.

체험 활동: 수업 토론 – 돈이란 무엇인가?

- ◆ 책상 위에 놓인 사탕을 아직 먹지 마세요.
- ◆ 누가 이 사탕을 1달러 지폐와 교환할 의사가 있나요?
- ◆ 이제, 사탕 대신 1달러짜리 모노폴리 지폐와 교환할 의사가 있는 사람은 계속 손을 들어주세요.
- ◆ 왜 그런가요? 또는 왜 그렇지 않은가요?
- ◆ 어떤 지폐는 그렇게 갖고 싶어지고, 다른 지폐는 쓰레기처럼 여겨지는 이유는 무엇인가요?
- ◆ 돈은 왜 “가치”가 있나요?
- ◆ 돈은 어디에서 오며, 누가 얼마나 발행할지를 결정하나요?
- ◆ 왜 더 많은 돈을 발행해서 모두에게 공평하게 나누어주지 않는 걸까요?

이 두 지폐의 차이는 한쪽이 다른 쪽보다 더 가치 있다고 믿는 것뿐입니다.



2.1 돈의 정의

한 번쯤 돈이란 무엇인지 깊이 생각해 본 적이 있나요? 대부분의 사람들은 돈을 사용하는 방법은 알고 있지만, 돈이 어디에서 왔는지 작동하는 방법을 잘 모릅니다. 돈은 본래 상품과 서비스를 교환하는 수단입니다. 이는 이러한 아이템들의 가치를 쉽게 거래할 수 있는 형태로 나타난 것입니다. 돈은 여러 가지 형태가 있습니다. 지폐, 금속 주화, 전자 결제가 그 예시입니다. 돈은 보통 정부나 다른 중앙 기관이 발행하고 통제하지만, 현실이나 온라인에서 교환 매체 이상의 의미를 가집니다. 돈은 세계 곳곳에 있는 사람들과 거래를 가능하게 해주는 널리 퍼져 있는 언어 와도 같습니다. 심지어 같은 언어를 사용하지 않거나 동일한 문화를 공유하지 않더라도 그렇습니다. 예를 들어 지구 반대편에 있어도 물건을 카운터 위에 놓고 현지 통화나 신용카드로 결제함으로써 돈이라는 “언어”를 사용할 수 있습니다.

제 2장

돈은 우리 소유물을 갖길 원하는 사람을 찾지 않아도 물물 교환이 가능하도록 해주는 사회 계약입니다. 만약 어떤 사람들이 초콜릿을 대부분의 상품과 서비스 대가로 받기 시작한다면, 초콜릿은 돈이 될 것입니다 (물론, 일부 지역에서는 초콜릿이 녹아버릴 수 있기 때문에 나쁜 돈으로 간주될 수도 있습니다).

프랑스 경제학자 장바티스트 세이는 “돈은 상품을 교환하는 그 순간에만 필요하며, 거래가 완료 되었을 때는 항상 어떤 한 종류의 상품이 다른 상품으로 교환되었음을 알 수 있다”고 말했습니다.

다시 말해, 돈 자체는 인간 욕구를 충족시킬 힘이 없으며, 단지 하나의 상품을 다른 상품으로 교환할 수 있게 해주는 도구일 뿐입니다.



거래란 재화와 서비스 교환 또는 이전을 의미합니다.
이는 당사자 간에 가치를 교환하는 방식입니다.

거래에는 여러 종류가 있으며, 간단한 교환 (예: 맥도날드에서 햄버거를 구매하는 것)부터 복잡한 금융 거래(예: 집을 구매하거나 주식 또는 채권에 투자하는 것)까지 다양합니다. 거래는 대면, 전화, 또는 온라인 등의 방법으로 이루어질 수 있으며, 개인, 기업, 금융기관 등 다양한 당사자가 관여할 수 있습니다.

돈이 없다면
이 거래가 쉬웠거나,
가능 했을까요?

소 한 마리를
100만 개의 딸기와
교환 하시겠어요?

그럼 60만 개
딸기는 어떨까요?
5만 개는요?



이 비디오를
확인해보세요.



돈은 재화가 교환되는 **수단입니다.**

돈은 재화가 교환되는 **목적이 아닙니다.**

요약하자면 돈은:

모든 사람들이 최종 결제 수단으로 받아들이기 때문에 거래를 용이하게 합니다. 또한, 가치를 측정하고 서로 다른 재화와 서비스를 비교할 수 있게 해줍니다. 이제 돈의 기능에 대해 살펴보겠습니다.

돈이란 무엇인가?

2.2 돈의 기능

돈은 우리가 필요한 물건을 사고파는 데 중요한 역할을 합니다. 돈은 다음과 같은 중요한 기능들을 수행합니다:

1 가치 저장

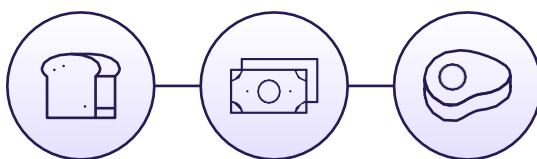
돈은 시간이 지나도 가치를 유지해야 하며, 노동 가치를 저장하고 미래에 투자 할 수 있도록 돋는 유용한 수단입니다. 이는 사람들이 돈을 사용해 미래를 계획하고, 돈을 빌리거나 빌려줄 수 있게 합니다. 그러므로 특별한 무언가를 위해서 돈을 저축한다는 것은 단순한 물건을 사는데 사용하는 것 이상의 의미가 있습니다. 돈은 여러분들 미래를 계획하고 투자할 수 있도록 돋는 도구입니다.

여러분은 어디에 가치를 저장 하시겠습니까?		 비트코인 (USD)	 금 (USD)	 달러 (EUR)
	2019년 3월 14일	\$3,846	\$1,293	€ 0.8817
	2020년 3월 14일	\$5,258	\$1,529	€ 0.90056
	이익/손실	+36.71%	+18.25%	+2.14%

2 교환의 매개체

돈이 존재한다면 여러분들이 가지고 있는 물건을 정확하게 원하는 사람을 찾을 필요가 없습니다. 그렇게 돈을 사용해 모든 것을 사고팔 수 있습니다. 이는 거래와 결제를 훨씬 더 편리하며 빠르고 알차게 만들어 줍니다.

교환의 매개체

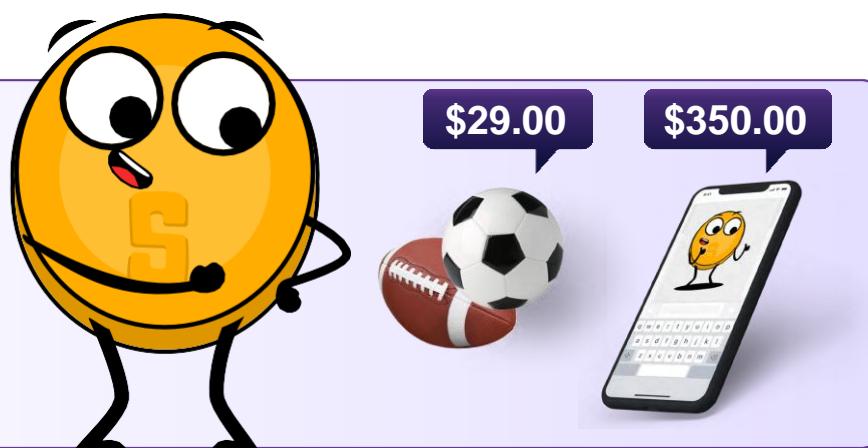


3 회계 단위

돈은 사람들에게 서로 다른 재화와 서비스 가격을 표현하고 비교할 수 있는 널리 퍼진 가치 기준을 제공합니다. 이는 더욱 알차고 투명한 시장이 형성되게 하여 무엇을 사고 팔지에 대해 현명한 결정을 내릴 수 있게 합니다.

회계 단위

소비자는 어떤 것에 가격 (화폐 가치)을 매길 때 그 가치가 얼마인지 알 수 있습니다.





제 2장

이렇게 생각해 보세요: 새 차를 사려고 할 때, 판매하는 대리점에 가서 표시된 차 가격을 비교하고 가격을 기준으로 어떤 차를 살지 결정을 내릴 수 있습니다. 만약 회계 단위가 없다면, 구매 하려는 자동차 가치를 다른 자동차와 비교하기 위한 어떤 기준을 사용해야 할 것입니다. 예를 들어 자동차 한 대의 가치가 소 몇 마리 가치인지 또는 자동차를 만드는 데 걸린 시간을 기준으로 비교해야 할 수도 있습니다.

이 세 가지 기능(교환 매개체, 회계 단위, 가치 저장)은 경제가 다양하고 활기 넘치게 발전할 수 있도록 해줍니다. 돈이 없다면 재화와 서비스를 사고파는 것이 훨씬 더 어려워지고, 우리의 경제는 덜 발전했을 것입니다.

수업 활동 - 이것은 돈의 어떤 기능일까요?

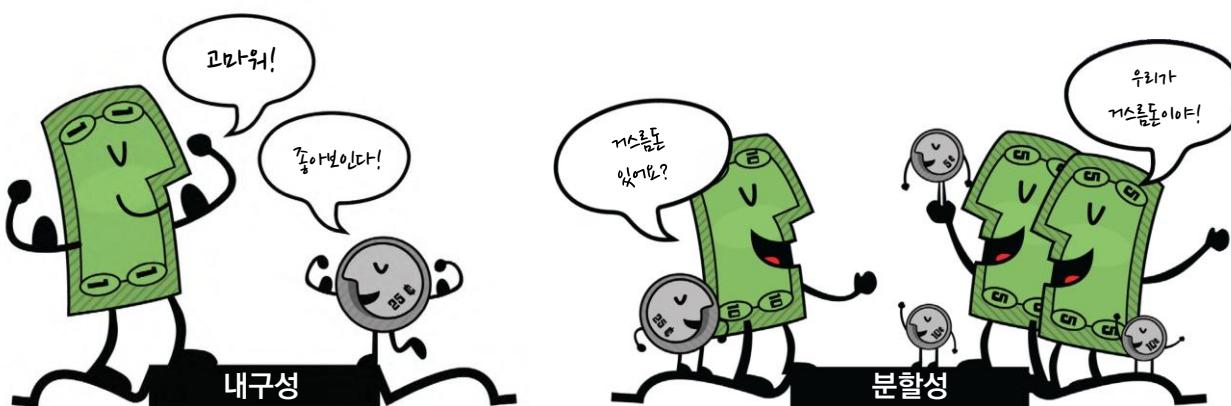
- ◆ 사토시는 강아지를 사려고 월급 일부를 저축하기로 결정했습니다.
- ◆ 사토시는 피자헛에서 8.30달러로 피자 두 조각을 샀습니다.
- ◆ 세일러는 75달러짜리 콘서트 티켓을 살지, 아니면 95달러짜리 스키 티켓을 살지 고민 중입니다.

2.3 돈의 속성

시간이 지나면서 사람들은 돈이 교환 매개체로 사용하기 위해서는 몇 가지 특성을 가져야 한다는 것을 깨달았습니다. 그 특성에는 내구성, 분할성, 휴대성, 수용성, 희소성, 그리고 대체 가능성이 있습니다.

◆ **내구성**은 돈이 외부에서 가해진 손상을 견디고 오랜 시간 동안 지속될 수 있는 능력을 의미합니다. 이는 돈이 경제에서 받아들여지고 인식 가능한 상태로 유통될 수 있도록 보장합니다. 금은 마모와 손상을 견딜 수 있는 소재로, 내구성이라는 돈의 특성을 잘 나타내는 좋은 예입니다.

◆ **분할성**은 더 작은 단위로 나누어 사람들이 다양한 금액으로 구매를 할 수 있게 합니다. 가격을 작은 단위로 쉽게 나눌 수 있어 돈이 가진 분할성을 잘 나타내는 좋은 예가 있습니다. 바로 우리가 사용하고 있는 지폐입니다.



돈이란 무엇인가?

휴대성은 돈을 쉽게 운반하는 것을 의미합니다. 이는 사람들이 돈을 사용하여 재화와 서비스를 사고파는 데 어려움이 없도록 해줍니다. 신용카드는 지갑이나 가방에 편리하게 넣고 다닐 수 있어, 휴대성이라는 돈의 특성을 잘 보여줍니다.



수용성은 돈이 결제 수단으로 널리 받아들여지는 것을 의미합니다. 이를 통해 사람들이 재화와 서비스를 자신 있게 사고팔 수 있습니다. 미국 달러는 널리 받아들여지는 결제수단이며, 돈의 수용성을 잘 나타냅니다.



희소성은 수량이 제한되어 있어 돈의 가치가 유지됩니다. 같은 양의 재화를 구매하기 위해 더 많은 돈을 쓰지 않아도 된다는 뜻입니다. 희귀하고 가치 있는 우표는 시간이 지나면서 가치가 올라가기 때문에 좋은 돈의 형태라 할 수 있습니다. 우표 수집가들은 종종 우표를 통해 돈을 투자해 다양한 포트폴리오를 구성합니다.



대체 가능성은 동일한 가치 단위 하나로 다른 단위의 돈과 교환할 수 있습니다. 돈은 일정해야 합니다. 주화는 그 크기와 무게가 동일해서 돈의 균일한 특성을 잘 나타냅니다. 1센트는 항상 1센트 가치를 가진다는 것이 그 예가 됩니다.



대체로 이러한 특성들은 무역과 상거래를 촉진하는 데 유용하고 쓸모 있는 도구이며, 경제 발전과 안정에 꼭 필요합니다.

제 2장



수업 활동

다양한 자산은 저마다 다른 특성을 가집니다. 돈의 기능 역시 자산마다 다릅니다. 우리는 결국 안정성, 희소성, 분할성, 이동성, 수용성들과 같은 특성을 바탕으로 어떤 자산을 돈으로 사용할지 결정합니다.

각각 특성에 다양한 항목이 얼마나 잘 부합하는지 판단해 봅시다. 항목별로 1에서 5까지 점수를 매길 수 있습니다. 각 항목의 점수를 합산하면 어떤 항목이 돈의 형태로 가장 적합한지를 결정할 수 있습니다.

[0 = 매우 나쁨, 3 = 보통, 5 = 매우 우수]

* 비트코인에 해당하는 칸은 채우지 마세요. 해당 내용은 나중에 강의에서 다룰 예정입니다.

다음 질문들을 활용하여 표에 있는 항목들이 돈의 특성에 얼마나 잘 부합하는지 평가해 보세요.

- 내구성:** 시간 흐름에 따라 마모와 손상을 견딜 수 있는가?
- 휴대성:** 쉽게 운반할 수 있으며 다양한 장소에서 사용할 수 있는가?
- 대체 가능성:** 다른 형태의 돈과 상호 교환이 가능한가?
- 수용성:** 널리 결제 수단으로 받아들여지는가?
- 희소성:** 희소하며 지나치게 풍부하지 않은가?
- 분할성:** 거래를 위해 더 작은 단위로 나눌 수 있는가?

좋은 돈의 특성	소	담배	다이아몬드	유로	비트코인
내구성					
휴대성					
대체 가능성					
수용성					
희소성					
분할성					
합산					

돈이란 무엇인가?

2.4 돈의 유형

돈은 실제 돈과 디지털 돈으로 나눌 수 있습니다.

실제 돈과 디지털 돈은 다음을 포함합니다:

- 명목화폐 (Fiat money): 정부가 발행하고 교환 수단으로 받아들여지는 지폐와 주화.
- 대안화폐 (Representative money): 실물 자산 청구권을 나타내는 화폐.
- 상품화폐 (Commodity money): 근본이 되는 가치가 있으며 교환 수단으로 널리 받아들여지는 상품(예: 금과 은).

모든 돈이
똑같지는 않다!

상품 화폐

화약은 한때
상품 화폐로
사용되었습니다.

대안 화폐

은 보증서와 같은
대안 화폐는 은으로
교환 할 수 있었습니다.

명목 화폐

오늘날, 연방준비제도도 발행
지폐는 명목 화폐이며,
연방 정부가 부채를 갚는데
사용 가능한 화폐입니다.

디지털 화폐는 온라인 거래에 사용될 수 있으며, 전자 화폐, 스테이블 코인, 암호화폐들을 포함합니다.

전자 화폐는 달러와 유로와 같은 기존 화폐 디지털 버전이며, 디지털 결제 시스템을 통해 온라인에서 물건을 사고파는 데 사용 할 수 있습니다.



결제 시스템은 전자 화폐와 기타 디지털 자산을 한 곳에서 다른 곳으로 이동시키는 데 필요한 인프라를 의미합니다. 그러나 기존 금융 시스템에서는 은행이나 기타 금융 기관과 같은 중개자가 항상 존재하며, 수수료를 부과하고 거래를 승인, 취소, 되돌리거나 지연시킬 수 있는 권한이 있습니다.



제 2장

금융 시스템에서 디지털 결제 시스템 주요 유형에는 카드 네트워크와 디지털 지갑이 포함됩니다. 카드 네트워크는 고객이 신용카드를 사용해 물건을 구매할 때 금융 기관과 판매자 사이의 자금 이동을 돋습니다. 그리고 디지털 지갑은 사용자가 전자 화폐를 저장하고 관리하며 자신의 계좌에서 돈을 받을 사람 계좌로 자금을 보내 결제를 할 수 있도록 하는 온라인 계좌입니다.



중앙은행 발행 디지털 화폐 (CBDC: Central Bank Digital Currency)

중앙은행에서 발행하고 보증하며, 정부가 중개하는 국가 법정화폐의 디지털 버전입니다.



스테이블코인

미국 달러와 같은 자산에 대해 일정한 가치를 유지하도록 설계된 디지털 화폐입니다.



암호화폐

디지털 화폐 한 종류로 비트코인은 분산화되어 코드로 운영되며, 다른 암호화폐는 중앙화되어 소수의 사람들이 통제합니다.

끝내 중개자 없이 작동하는 화폐는 소수가 화폐 공급을 독점하고 권력을 집중시키는 것을 방지하기 때문에 사회를 더 알차고 이롭습니다. 하지만 당사자 간 신뢰에 의존하지 않으면서도 안전한 거래를 가능하게 하는 화폐를 만드는 것은 인류 역사상 어려운 과제였습니다. 이것을 위해 인터넷처럼 모든 사람이 동등한 통제권을 가지면서도, 중앙화 된 권력이 개입하지 않는 방식으로 운영되는 화폐가 필요합니다. 이를 위해서는 권력을 가진 사람들을 포함한 모든 당사자들이 더 큰 이익을 위해 통제권을 포기한다는 합의가 필요합니다.

돈이란 무엇인가?

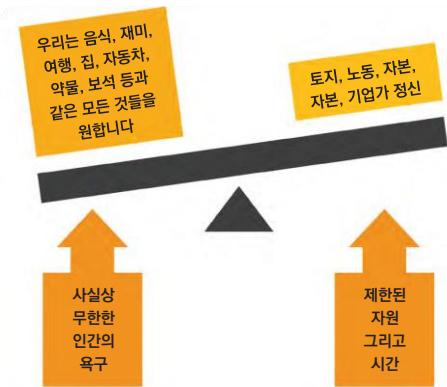
2.5 돈의 심리학: 희소성, 시간 선호, 트레이드-오프

여러분이 사막에 고립되어 있고, 물 한 병만 남아 있다고 상상해 보세요. 목이 마르고 당장 물을 마시고 싶지만, 더 많은 물을 찾을 때까지 살아남으려면 이 물이 필요하다는 것도 알고 있습니다. 이것은 희소성의 좋은 예입니다. 즉, 제한된 자원(물)만 있으며, 언제 사용할지 선택해야 하는 상황입니다. 이러한 상황에서는 조금씩 물을 아껴 마시며 최대한 오래 버티려고 할 것입니다.



희소성은 우리가 자원 사용 선택을 고민하게 만들고, 그 과정에서 장단점을 따져보며 선택의 대가(트레이드-오프)를 받아들이도록 합니다.

또는 한 번에 최대한 많은 물을 마셔서 더 많은 물을 찾을 에너지가 생기기를 바랄 수도 있습니다. 결국, 당장의 갈증을 해소할지 아니면 나중에 마시려고 물을 아껴둘지 선택해야 하며, 어떤 선택을 하든 어려운 결정을 마주하게 됩니다. 이러한 희소성 개념은 물 뿐만 아니라 모든 종류의 자원에 적용됩니다. 돈, 시간, 심지어 사랑과 관심조차도 우리는 항상 제한된 자원을 올바르게 선택하는 방법을 마주하고 있습니다.



희소성의 두 가지 유형: 인간이 만든 희소성과 자연에서 나온 희소성.

- 인간이 만든 희소성, 즉 집중형 희소성에는 한정판 디자이너 가방, 희귀 스포츠 카드, 번호가 매겨진 예술품 등이 있습니다. 이러한 것들은 쉽게 복제되거나 위조될 수 있습니다.
- 자연에서 생겨난 희소성, 즉 분산형 희소성에는 소금, 조개, 금과 같은 귀금속이 포함됩니다. 이러한 것들은 복제하거나 위조하기가 어렵습니다. 두 가지 주요 차이는 통제 여부입니다.

집중형 희소성은 기업이나 정부와 같은 단일 기관이 통제하며, 분산형 희소성은 누구의 통제도 받지 않습니다. 가난한 사람들에게 더욱 영향을 미치는 집중형 희소성의 예로는 깨끗한 물과 같은 필수 자원 통제가 있습니다. 일부 지역에서는 깨끗한 물을 민간 기업이나 정부 기관이 관리하며, 제한하거나 통제 할 수 있어 중요한 자원은 매우 귀해집니다. 그러므로 이러한 통제는 물 가격이 오르게 하거나 깨끗한 물에 대한 접근을 막게 되므로, 결국 가난한 사람들이 가장 큰 영향을 받습니다. 깨끗한 물 통제는 이들의 건강과 복지에 영향을 미칠 뿐만 아니라, 더 비싼 물값을 지불하거나 먼 거리를 이동해 물을 구해야 하는 상황을 만들어 빙곤을 지속시킵니다.

희소성은 우리 선택에 영향을 미치며, 희소성을 이해한다면 더 나은 의사결정을 할 수 있습니다. 우리는 종종 바로 앞에 놓인 이익과 오랫동안 이어지는 이익 사이에서 선택해야 하며, 이러한 트레이드-오프는 우리가 목표를 달성하는 길을 만들어 줍니다.



제 2장



시간 **선후**란 사람들이 어떤 것을 미래보다 현재에 더 갖고 싶어하는 성향을 의미합니다.



시간 선후의 예:

오늘 \$100을 받거나 1년 후 \$110을 받을 수 있는 선택지가 있다고 가정해봅시다. 만약 여러분이 높은 시간 선후를 추구 한다면, 1년 동안 기다려서 추가 \$10을 받는 것보다 지금 당장 \$100을 받는 것을 더 가치있게 여길 수 있습니다. 반면에 낮은 시간 선후를 추구 한다면, 더 큰 보상을 받으려고 기다리는 것을 선호할 것입니다. 이는 곧바로 느끼는 만족보다는 오랜 기간 계획에 더 집중하기 때문입니다.

체험 활동: 시간 선후

높은 시간 선후 vs 낮은 시간 선후

- 1 선생님의 사탕 선택 게임에 대한 설명을 들으세요.
- 2 지금 사탕 1개를 받을지, 아니면 수업이 끝난 후 사탕 2개를 받을지 결정하세요.
- 3 결정을 확정하고 선생님께 선택을 알리세요. 선택에 따라 사탕을 즉시 받거나 수업이 끝날 때 받으세요.
- 4 수업 토론에 참여하여, 의사 결정 과정과 시간 선후 개념에 대해 되돌아보세요.

결론 및 토론

- ▶ 여러분이 지금 사탕을 받거나 나중에 더 큰 보상을 기다리기로 한 결정에 영향을 준 요인은 무엇인가요?
- ▶ 이 활동이 끝난 지금, 결정에 대해 어떻게 느끼시나요?
- ▶ 높은 시간 선후가 해로울 수 있는 상황과 낮은 시간 선후가 유익할 수 있는 상황의 실제 사례를 생각해볼까요?
- ▶ 낮은 시간 선후보다 높은 시간 선후를 선택했을 때의 결과는 무엇인가요?

사막 예시에서, 나중을 위해 물을 남기는 것보다 당장 모든 물을 마시고 싶어질 수 있음을 의미합니다. 지금 느끼는 갈증이 미래에 느낄 수도 있는 갈증보다 더 절박하기 때문입니다.

반면에 물을 아껴서 천천히 마시기로 결정한다면, 여러분 시간선후도는 낮다고 할 수 있습니다. 즉 시간을 기다리면서 생존 가능성을 높이는 것을 선택한 것입니다.

돈이란 무엇인가?



기회비용은 결정을 내릴 때 포기하는 차선책의 가치를 의미합니다. 모든 결정에는 트레이드-오프가 따릅니다.

오늘의 선택



딸기스무디에
7달러를 쓰기

현재



다른 곳에 7달러를 쓰기

미래



7달러를 일정한 주기로
저축하여 얻은 혜택

사막 예시에서 물을 한꺼번에 마시는 것의 기회비용은, 물을 아껴 사용하며 더 긴 시간 동안 얻을 수 있었던 생존의 이점입니다.

예를 들어 물을 아껴서 오랜 시간 동안 조금씩 마시기로 결정했다고 가정해 봅시다. 그러면 더 많은 물을 찾기 위해 필요한 에너지와 수분을 유지할 수 있습니다. 물을 찾는 동안 약간의 물이 들어 있는 선인장을 발견하게 됩니다. 물은 많지 않지만, 당장의 갈증을 해소하기에는 충분합니다. 만약 처음에 물을 한꺼번에 마셨다면, 더 많은 물을 찾기 위한 에너지가 부족해 선인장을 발견하지 못했을 수도 있습니다.

물을 한꺼번에 마신 것의 기회비용은 선인장을 발견하고 추가 수분을 얻을 기회를 잃는 것이었을 것입니다.

이 예시는 기회비용이 단순히 두 가지 선택 사이에서 바로 나타나는 트레이드-오프 뿐만 아니라, 우리 선택으로 인해 얻거나 잃을 수 있는 미래의 기회도 포함한다는 점을 보여줍니다.

미래의 더 큰 보상을 포기하고 지금의 작은 보상을 선택하는 우리 의지는 시간 선호에 영향을 받습니다. 이는 바로 느끼는 만족과 오래 두고 볼 계획 중 어느 쪽을 더 가치 있게 여기는지에 따라 달라집니다.

이 장에서는 돈의 기본 개념, 정의, 기능, 속성 및 다양한 유형을 탐구했습니다. 논의의 핵심은 희소성, 시간 선호, 그리고 트레이드-오프와 같은 개념에 초점을 맞춘 돈의 심리를 이해하는 것입니다. 이러한 탐구는 돈의 복잡한 본질과 우리의 삶에서 그 역할을 이해하는 데 기초를 마련했습니다. 다음 장에서는 돈의 역사와 시간이 지나면서 발전한 역사에 대해 이야기할 것입니다.

제 3장

돈의 역사

3.0 서론

체험 활동: 물물교환 게임

3.1 물물교환에서 현대 화폐로 진화

3.1.1 초기 화폐 문제점

3.1.2 주화와 지폐의 발달

3.1.3 건전화폐에서 불건전화폐로 전환

3.1.4 지폐에서 플라스틱카드로

3.2 디지털 화폐

돈의 역사

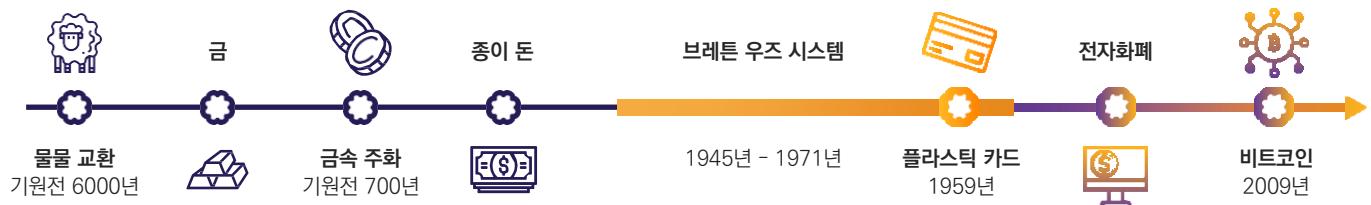
3.0 서론

“

화폐는 계획을 통하여 발전된 것이 아니라 자유시장에서 생겨났습니다.
이는 정부가 만든 것이 아니며, 시간이 흐르면서 자연스럽게 등장한 것입니다.

머레이 로스바드

”



사람들이 오늘날 우리가 사용하는 주화나 지폐를 갖고 있지 않았던 아주 오래전 시절을 상상해 보세요. 그 당시에는 조개껍데기나 금과 같은 귀금속을 특별한 화폐로 사용하며 물건을 교환했습니다. 이게 조금 낯설게 들릴 수 있지만, 그것이 그 당시의 화폐였고 모두가 그 가치를 인정했습니다. 이번 장에서는 시간 여행을 통해 화폐의 진화를 직접 경험하고, 그 기원을 추적하며 역사를 거치면서 변화하고 적응해온 방법을 살펴볼 것입니다.

체험 활동 – 물물교환 게임

선생님께서 작은 종이를 하나 나눠 주셨습니다. 이 게임에서 여러분의 목표는 역사 속 상거래를 통해 자신이 '가진 것'을 자신이 '원하는 것'으로 교환하는 것입니다. 종이 위에 이름을 작고 알아보기 쉽게 적어 주세요.

💡 라운드 1: 물물교환

지금은 기원전 6000년입니다. 우리가 알고 있는 화폐는 아직 발명되지 않았습니다.
여러분은 메소포타미아에 있으며, 물건과 서비스를 서로 **물물교환**으로 직접 교환하고 있습니다.



참고로 현재도 일부 기업은 서비스에 대해 비화폐 결제를 허용하며 정부는 이러한 물물교환 거래를 세금 신고 목적으로 화폐 거래와 동일하게 취급합니다."



첨선 부분에서 종이를 잘라 주세요. 여러분의 목표는 '가진 것'을 계속 교환하여 끝내 '원하는 것'을 얻는 것입니다.
처음 정한 '원하는 것'을 변경할 수는 없습니다. 목표를 달성하기 위해 여러분에게 주어진 시간은 5분입니다.

제 3장



새로운 “물건”이 처음 원했던 “원했던 것”과 일치하면 자리로 돌아가세요. 시간이 다되면 물물교환 상대를 찾지 못했더라도 자리로 돌아가세요.



한 번의 물물교환 거래로 원하는 것을 얻은 사람은 손을 들어보세요.

다음 질문에 간결하면서도 최선을 다해서 답변 해보세요:

1. 왜 어떤 사람들은 물물교환 거래 상대를 찾을 수 있었고, 다른 사람들은 못 찾았을까요?

2. 물물교환의 장점은 무엇인가요?

3. 직접 경험해본 물물교환의 단점은 무엇인가요?



라운드 2: 상품화폐

시간을 빠르게 돌려 기원전 14세기경 서아프리카 해안으로 가봅시다. 물물교환은 점점 번거롭고 시간이 많이 들게 변했습니다. 우리는 문명이 발전하며 이제 **상품 화폐**(commodity money)를 사용하고 있습니다.

조개껍데기에서 주화까지



기원전 1300년



기원전 1000년



기원전 687년

이 초기 주화는 타원형이었으며, 금과 은의 합금인 일렉트럼으로 만들어졌고, 한쪽 면에만 새겨져 있었습니다.



재밌는 사실

카우리 조개껍데기는 20세기까지 아프리카 일부 지역에서 법정화폐로 사용되었습니다.

기원전 1300년

카우리 조개껍데기가 아시아, 아프리카, 오세아니아 및 유럽 일부 지역에서 주요한 지불 수단으로 사용되었습니다.

기원전 1000년

중국 서주(西周) 왕조가 금속 화폐를 사용하기 시작했습니다.

기원전 687년

리디아(현재의 터키) 왕국의 알리아테스 왕이 서양에서 최초로 금속 화폐 주화를 주조합니다.

돈의 역사

선생님께서 여러분에게 쌀 한줌(또는 쌀 한줌을 출력한 이미지)를 주셨습니다. 각 상품의 가격이 쌀 한줌이라고 가정해 봅시다.

여러분의 목표는 “원하는 물건”을 얻는 것입니다. 하지만 이번에는 우리가 조금 더 똑똑해져 특정 문제를 해결할 방법을 찾았습니다.

- 💡 왜 쌀 한줌을 상품 화폐(commodity money)라고 간주할까요?
 - 💡 이제 원하는 물건을 얻을 수 있나요?
 - 💡 쌀 한줌을 사용하는 이번 거래가 더 쉬웠나요?
 - 💡 왜 돈이 상품을 대신하게 되었을까요?
 - 💡 상품 화폐를 사용하는 것이 물물교환보다 더 편리한 이유는 무엇인가요?
 - 💡 쌀 한줌을 화폐로 사용하는 데에는 어떤 단점이 있을까요?
 - 💡 일본이 아주 많은 쌀(일본에서 한국으로 가져온 금과 은)을 여러분에게 가져오기 시작했을 때 어떤 일이 일어났을 것이라고 생각하나요?
-
-
-

3.1 물물교환에서 현대 화폐로 진화

3.1.1 초기 화폐 문제점



이 짧은 영상을 시청하여 “교환의 역사”에 대해 알아보세요. “종이 화폐의 역사” 시리즈의 일부입니다.



물물교환 경제에서는 사람들이 자신이 제공할 수 있는 상품과 서비스를 비교한 가치 기준으로 서로 거래를 합니다. 그러나 물물교환 경제는 효율이 떨어지며, 현재처럼 복잡한 사회에서는 관리하기 어렵습니다.

물물교환 시스템에서는 **쌍방 요구 일치(double coincidence of wants)**가 필수입니다. 즉 상대방이 원하는 것을 내가 갖고 있으면서, 동시에 내가 원하는 것을 상대방이 제공해야 거래가 성립됩니다.

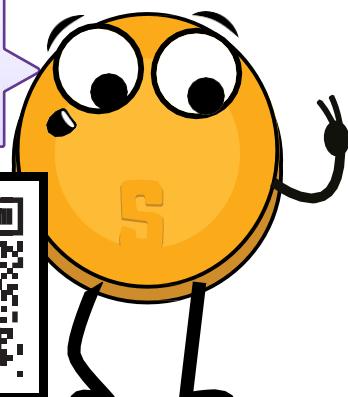
제 3장



다음 상황을 가정해 봅시다:

- ◆ 사토시는 바나나를 세일러의 코코넛과 교환하고 싶어 합니다.
- ◆ 하지만 세일러는 코코넛을 로라의 망고로 교환하고 싶어 합니다.
- ◆ 그런데 로라는 망고를 사토시의 바나나로 교환하려고 합니다.
- ◆ 결국 그들은 쌍방 요구 일치(double coincidence of wants)가 이루어지지 않아 끝없는 과일 물물교환 순환에 갇히고 맙니다.
- ◆ 사토시는 과일 대신 시원한 탄산음료로 교환하자고 제안하지만, 자신들이 외딴 섬에 있어 탄산음료가 없다는 사실을 깨닫습니다.
- ◆ 결국 모두 조용히 해변에 앉아 각자 과일을 즐기기로 합니다.

이것은 종이 화폐의 역사 시리즈의 두 번째 에피소드로, 제목은 “단순한 국수가 아니다”입니다.



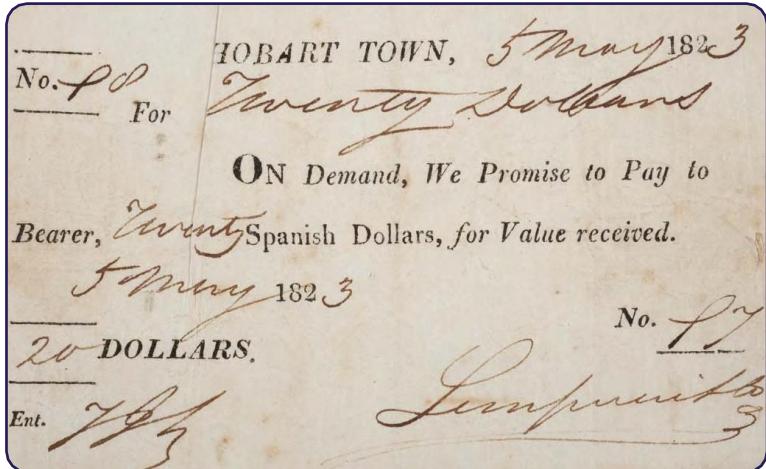
3.1.2 주화와 지폐의 발달

여러분들의 공동체가 무역과 상거래에 더 깊이 관여하게 되면서, 물물교환이나 그 밖에 화폐가 아닌 교환 방식의 한계를 깨닫게 됩니다. 이에 다른 화폐 형태 중 하나로 금속 주화를 사용하기로 결정합니다.



상품 화폐는 금과 은과 같은 귀금속 재료로 만들어진 화폐를 말합니다. 이러한 화폐는 오랜기간 가치 저장 수단, 교환 매개체, 그리고 회계 단위로 사용되었습니다.

돈의 역사



이들은 금과 같은 귀금속을 담보로 발행되었으며, 17세기부터 19세기까지 실제 금속으로 교환이 가능했습니다. 이를 통해 더 휴대하기 쉽고 편리하게 거래할 수 있는 화폐를 사용할 수 있게 되었으며, 귀금속의 가치와 안정성을 유지할 수 있었습니다.

그러나 금속 주화를 더 많이 사용하면서 몇 가지 단점을 발견하게 됩니다. 주화는 대규모 거래에서 무겁고 휴대하기 불편할 수 있으며, 일부 사람들이 주화를 녹여 값싼 금속을 섞어 새로운 동전을 만들어내는 방식으로 시스템을 악용하고 있다는 점을 알게 됩니다. 이러한 행위는 물건 가격의 상승을 초래하고, 화폐 시스템에서 신뢰를 떨어뜨립니다.

여러분들은 이러한 문제를 해결하려고 화폐 차용증을 화폐의 한 형태로 사용하기 시작합니다. 이러한 화폐 차용증은 고대 중국에서 시작됐으며, 편리하고 쉽게 교환할 수 있는 화폐입니다.



3.1.3 건전화폐에서 불건전화폐로 전환

17세기 스웨덴으로 시간을 빠르게 돌려봅시다. 이제 여러분들은 귀중한 자산을 은행에 오롯이 의존하여 보관하고 있습니다.

그러나 점점 수상한 일이 벌어지고 있음을 깨닫게 됩니다. 은행들이 보유한 금보다 더 많은 화폐 차용증을 발행하고 있는 것처럼 보입니다. 이는 보유한 자산보다 더 많은 돈을 창출할 수 있게 해주는 행위입니다.

은행들은 이러한 교묘한 수법을 통해 고객이 보관 중인 금의 가치와 화폐 차용증의 가치 차이에서 이익을 얻을 수 있습니다.



지폐 제도를 실제로 실행하려 하면 어떤 일이 벌어질까요?
“종이 화폐의 역사” 시리즈
네 번째 에피소드에서 확인해보세요.



여러분들은 지금이 화폐의 작동 방식이 크게 변화하는 순간임을 깨닫습니다. 과거에는 건전화폐(sound money), 즉 귀금속으로 담보된 화폐 시스템을 사용했지만, 이제는 불건전화폐(unsound money), 즉 실물 자산으로 뒷받침되지 않는 명목화폐(fiat currency) 시스템으로 전환되고 있습니다. 이러한 변화는 하루아침에 이루어진 것이 아니라 점차 나아지는 과정이었습니다. 산업 혁명으로 인한 대량 생산과 도시화, 은행과 주식 시장 같은 고도화된 금융 시스템의 성장이 이 과정에 영향을 미쳤습니다. 또한 중앙은행의 등장으로 화폐를 중앙집권화하여 통제를 강화했으며, 경제 성장을 지원하려고 명목화폐를 발행하는 체제로 전환하는 계기가 되었습니다.

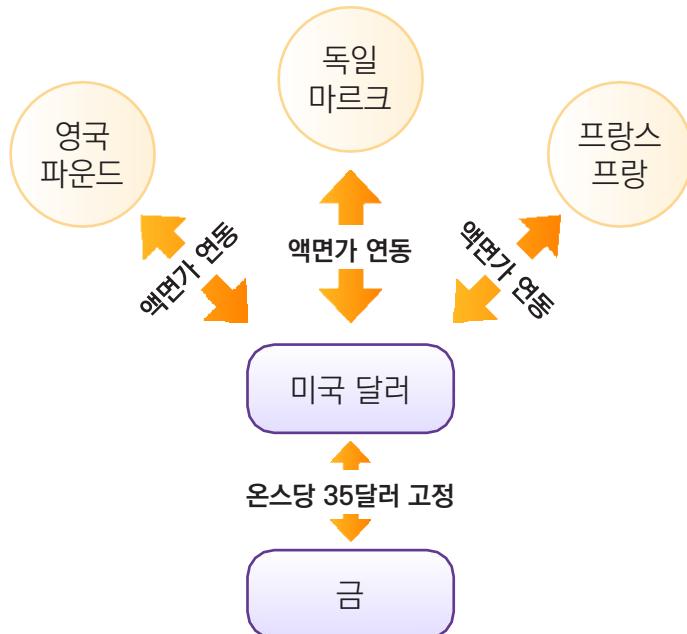


그러나 점점 이러한 **중앙집권화가 갖는 단점**도 보이기 시작합니다.
그 중에는 무분별한 소비, **증가하는 부채**, 그리고 경제 발전을 이루려고 한다는 이유로 시민을 통제합니다.

제1차 세계대전 이전까지, 당신은 지폐를 정해진 양의 금으로 교환할 수 있었습니다. 그러나 두 차례의 세계대전과 1929년 경제 대공황이 이 시스템을 종식시켰습니다. 1944년 브레튼우즈 협정이 체결되면서 미국 달러가 세계 기축통화로 자리 잡았으며, 달러의 가치는 금 가격에 온스당 35달러로 고정되었습니다. 다른 국가들의 화폐는 미국 달러에 연동되었으며, 이는 국제 금융 시장의 안정화에 기여했습니다.

브레튼우즈 시스템

(1945 – 1972)



그러나 안타깝게도 이 시스템은 1960년대 후반부터 균열이 생기기 시작했고 결국 1971년 닉슨 쇼크로 이어졌습니다. 당시 미국 정부는 달러의 금태환을 중단했으며 이는 금본위제의 종말과 부채로 만들어낸 신용화폐 시스템 중심의 세계가 시작됨을 의미했습니다.

점점 돈의 가치가 예전 같지 않음을 실감하게 됩니다. 길이가 계속 변하는 자로는 테이블의 길이를 정확히 측정하기 어려운 것처럼, 명목화폐 시스템에서는 권력을 가진 자들의 결정에 따라 화폐 가치가 예측할 수 없이 변동되기 때문에, 상품과 서비스의 가치를 정확히 측정하기 어려워집니다.

더 이상 금과 같은 실물 자산에 연동되지 않는 화폐 가치에 적응하면서 혼란과 불안을 느끼게 됩니다.

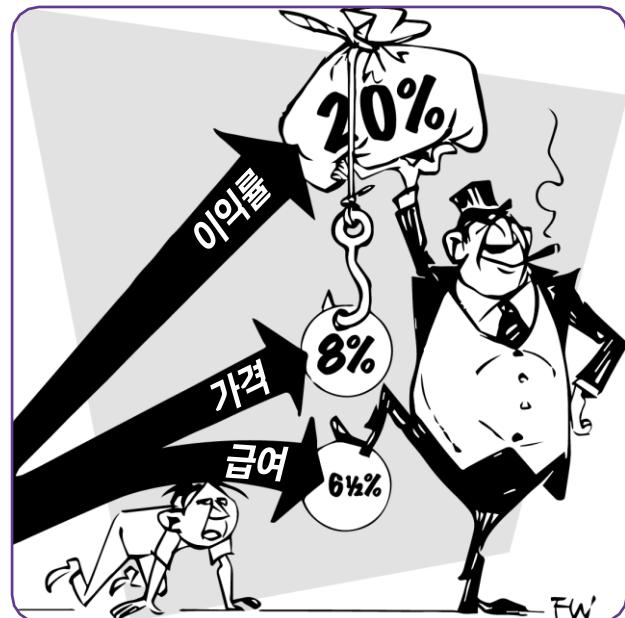
돈의 역사

여러분들은 이러한 변화가 세계 경제에 미치는 영향을 목격하며, 명목화폐 안정성과 신뢰성에 대해 의문을 갖기 시작합니다. 또한 달러가 금에 고정되어 있던 시절처럼 일관된 가치를 유지하지 않고 변동성을 갖게 되었음을 깨닫습니다. 이로 인해 달러를 회계 단위(unit of account)로 사용하기가 더 어려워지며, 그 가치는 인플레이션(물가 상승), 금리, 국가 경제 상황, 정치, 시장 투기, 국제 무역 수요 같은 다양한 요인들에 영향을 받게 됩니다. 달러가 갖는 가치가 끊임없이 변동하는 상황 속에서 일상 생활에 미치는 영향을 파악하고 살아가는 것이 점점 더 혼란스럽고 예측하기 어려운 시대가 되었음을 실감하게 됩니다.

현대 화폐 시스템을 통해 삶의 질을 향상시키려는 노력, 효율성 증대, 정보 접근성 향상, 소통의 발전 등이 이루어졌지만, 사람들의 생활 수준은 점차 하락하기 시작합니다.

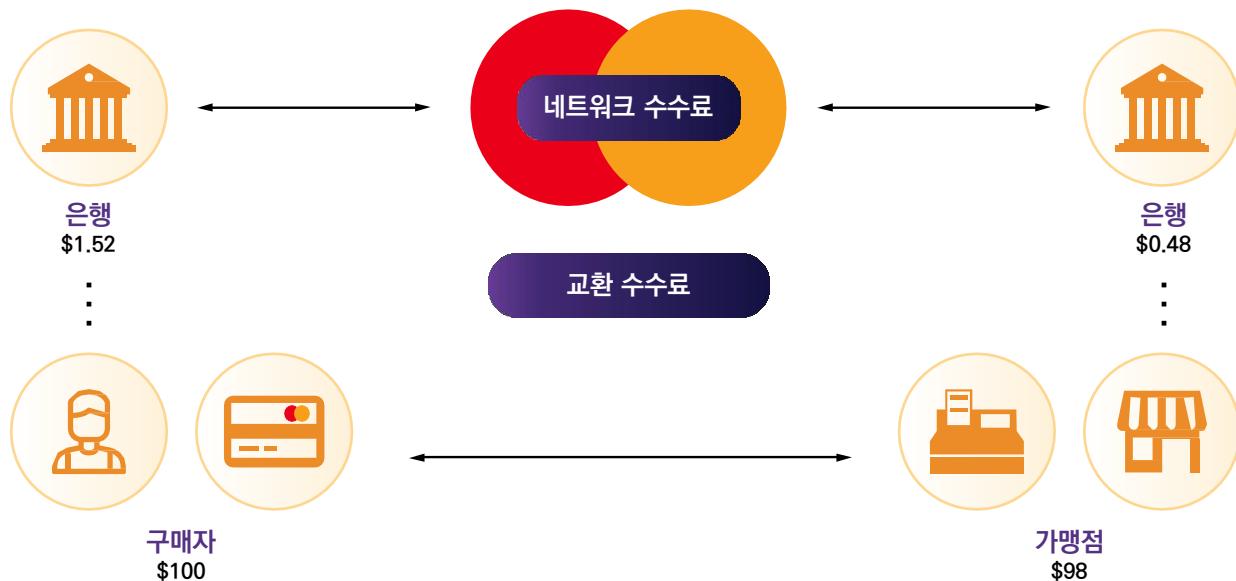
- ◆ 중앙집권 통제의 남용
- ◆ 끊임없는 물가 상승
- ◆ 정체된 실질 임금
- ◆ 약화되는 화폐 가치
- ◆ 더 적은 것을 얻으려면, 더 많은 돈을 지출해야 하는 상황

이로 인해 가난한 사람들은 교육, 신용, 금융, 복지, 사회 네트워크 등이 제한되며, 결국 돈을 벌 수 있는 기회조차 불리한 상황에 놓이게 됩니다. 그 결과 부자는 더욱 부유해지고, 가난한 사람들은 더욱 가난해지는 현상이 지속됩니다.



3.1.4 종이에서 플라스틱으로

오늘날 우리는 1950년대 첫 번째 신용카드가 도입된 이후로 먼 길을 걸어왔습니다. 간단히 플라스틱 카드를 한 번 짚는 것만으로도 원하는 것을 언제든, 어디서든 번거로움 없이 구매할 수 있습니다. 마치 끝없는 가능성의 세계를 여는 것 같고, 그 안에 무엇이 있는지 발견하는 설렘이 생생하게 느껴집니다… 적어도 우리는 그렇게 생각했습니다. 그러나 신용에 대한 의존이 고통스러운 후유증을 남길 것이라는 점을 알지 못했습니다. 예를 들면 모든 상품의 가격 상승과 결국 실패할 수밖에 없는 경제 구조를 조장하는 문제와 같은 것들입니다.



기술이 발전함에 따라 돈을 다루는 방식도 함께 변화하고 있습니다. 인터넷은 금융에서 중요한 역할을 하게 되었으며, 온라인 뱅킹과 전자상거래 웹사이트를 통해 온라인에서 돈을 직접 관리하고 사용할 수 있는 환경이 조성되었습니다.

디지털 화폐 등장은 이러한 변화 속에서 또 하나의 중요한 도약을 의미하며, 새로운 가능성을 열어주고 금융 거래 방식 자체를 변화시키고 있습니다.

3.2 디지털 화폐

기존 화폐와 달리, 디지털 화폐는 온라인으로만 존재합니다. 디지털 화폐는 컴퓨터와 소프트웨어를 통해 저장되고 교환됩니다.

디지털 화폐는 사람들이 인터넷을 통해 돈을 송금할 수 있도록 해줍니다. 이메일이 메시지를 즉시, 배송비 없이 보낼 수 있는 것처럼 디지털 화폐도 가치를 빠르고 매우 적은 비용으로 주고받을 수 있게 합니다.

오늘날 우리가 사용하는 화폐는 점점 더 디지털화되고 있습니다. 전체 화폐 밸런스 중 주화나 지폐 비율은 아주 작습니다. 은행과 금융 서비스는 사용자들이 인터넷을 통해 돈을 쉽게 교환할 수 있는 어플리케이션을 제공합니다. 그런데 이 돈은 어디에서 오는 걸까요?

이번 장에서는 금으로 대표되는 건전화폐(sound money)에서 종이로 된 불건전화폐(unsound money)로, 그리고 현재 디지털 법정화폐로 가려는 변화를 확인했습니다. 다음 장에서는 현재의 명목 화폐 시스템이 작동하는 방법, 그리고 그것이 형성된 역사를 탐구할 것입니다.

제 4장

명목화폐란 무엇이며, 누가 통제하는가?

4.0 서론

4.1 명목화폐의 간략한 역사

4.2 명목화폐 시스템

4.2.1 법령에 의한 화폐 시스템

4.2.2 은행 부분지급준비 제도: 부채로 운영되는 시스템

체험 활동: 은행의 부분지급준비 제도

4.2.3 누가 명목화폐 시스템을 통제하며, 이익을 얻는 방법은 무엇인가?

4.3 중앙은행 디지털 화폐(CBDC): 명목화폐의 미래

학습 워크북

한국어 버전 | 2025

명목화폐란 무엇이며, 누가 통제하는가?

4.0 서론

인류 역사란 곧 돈의 가치가 하락해 온 역사이다.

밀턴 프리드먼

이전 장에서 우리는 돈이 시간이 흐르며 변화한 역사, 그리고 우리 화폐 시스템이 건전화폐에서 불건전화폐로 전환되며 오늘날의 세계를 형성하게 된 과정을 살펴보았습니다. 이번 장에서는 이러한 변화가 현재 명목화폐(fiat currency) 시스템으로 진화했는지, 그리고 운영되는 방법을 더 깊이 탐구할 것입니다.

그렇다면 현재 명목화폐 시스템은 어떤 모습이며, 어떻게 탄생하게 되었을까요?

이 질문에 답하려면 먼저 세계 기축통화인 미국 달러(USD)에 주목해야 합니다. 오늘날 미국 달러는 글로벌 경제에서 중요한 역할을 하며, 이 결정은 모든 국가에 영향을 미칩니다. 따라서 국가에서 명목화폐 시스템이 운영되는 기초부터 이해하려면 이것이 시작된 화폐 역사를 파악하는 것이 필수입니다.

4.1 명목화폐의 간략한 역사

1815 – 1933	1913	1933	1934	1944	1971	1980
금 스탠다드	연방준비제도 (FED) 라고 불리는 중앙은행 설립	모든 국민은 온스당 \$20.67 환율로 금을 정부에 강제로 반납	달러 가치를 40% 절하하여 금을 1온스당 \$35로 조정함으로써 국민의 부를 강탈	브雷頓우즈 협정: 미국 달러(USD)가 세계 기축통화 확정	미국 달러 금 태환 중단으로 명목 화폐 (fiat system) 탄생	1970년 금 1온스당 \$35에서 1980년 \$870로 급등하여 불과 10년 만에 화폐 가치가 96% 하락

한눈에 보는 타임라인

19세기 전 세계 문명은 건전화폐 스탠다드로 금과 은과 같은 귀금속이 희소성, 내구성, 인식 가능성 때문에 화폐로 사용되었습니다. 그러나 세계 무역이 등장하면서, 많은 금속을 운반하는 것이 어려워졌고 금·은 보관 창고가 등장하게 되었습니다. 이 창고들은 사람들이 맡긴 귀금속을 보관했으며 그 만큼 금 또는 은으로 교환 가능한 화폐 차용증을 발행하였습니다. 사람들은 돈(귀금속)을 예치하는 대가로 지폐를 받게 되었습니다.

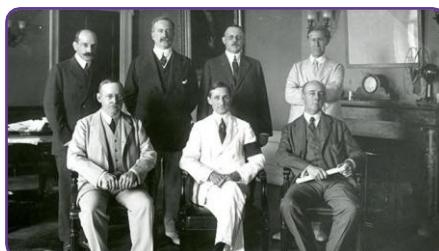


제 4장

이 증서들은 보관된 금이나 은의 정확한 양과 정확하게 연결되어 있었습니다. 이러한 종이 증서와 실물 상품 화폐가 직접 연결되어 있는 형태는, 오늘날 우리가 은행이라 부르는 제도의 초기 형태를 이루었습니다.



은행은 고객들의 돈을 안전하게 보호하는 것을 목표로 했지만, 차츰 무분별한 대출을 일으키려고 고객의 돈에 손을 대기 시작하면서 보유하지 않은 금의 증서를 발행했습니다. 이러한 관행은 많은 고객이 동시에 돈을 찾으려 할 경우 은행이 무너지는 “뱅크런”의 위험을 초래했습니다. 뱅크런을 막기 위해 은행들은 정부와 협력하여 재대출을 합법화하는 시스템을 구축했습니다.

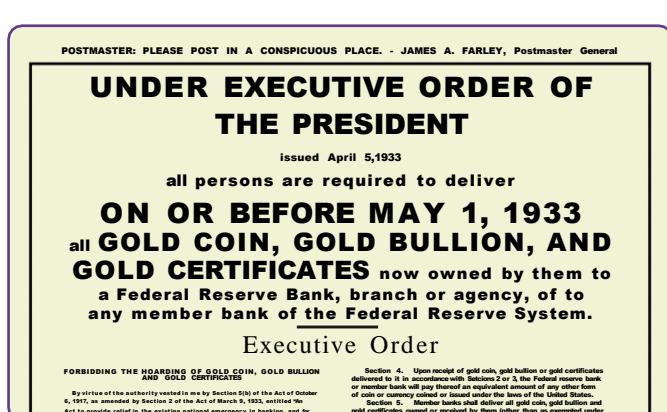


1913년에는 중앙은행인 연방준비제도(Federal Reserve)를 설립하여 새로운 지폐를 발행하고 위기에 처한 은행들을 구제하는 역할을 맡게 되었습니다.

전 세계 정부들은 금과 은의 가치를 깨달으면서 차지하기 위한 전쟁이 벌어졌습니다. 제2차 세계대전 무렵, 레닌, 스탈린, 처칠, 루스벨트, 무솔리니, 히틀러와 같은 지도자들은 금을 확보하기 위한 목적으로 움직였습니다.

1930년대 초반, 미국에서 화폐를 뒷받침하는 자산에 중요한 변화가 발생했습니다. 당시 많은 사람들의 재산은 금으로 보관되고 있었습니다. 그러나 1933년, 프랭클린 루스벨트 대통령은 행정명령 6102호를 발령하여 모든 국민에게 가진 금을 정부에 넘겨줄 것을 요구했습니다. 이는 사람들이 스스로 교환한 것이 아니었으며, 금을 내놓지 않을 경우 심각한 처벌을 받을 수 있었습니다.

정부는 금 1온스당 20.67달러의 환율을 정했습니다. 즉, 개인이 가진 금 1온스당 20.67달러 상당의 종이 증서를 받게 되었습니다. 사람들은 언젠가 종이 달러로 금으로 교환할 수 있을 것이라는 희망을 가지고 순응해야만 했습니다.

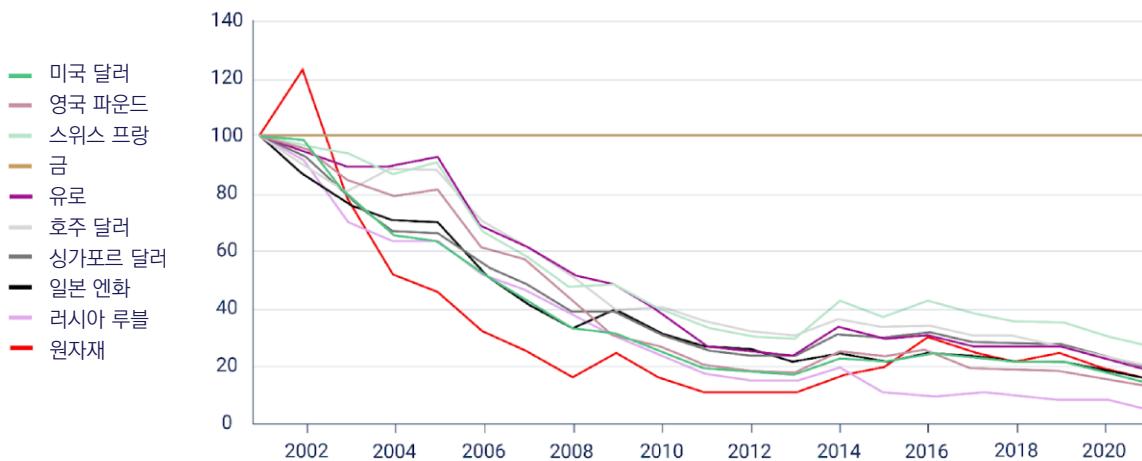


명목화폐란 무엇이며, 누가 통제하는가?

1934년 금 비축 법안이 제정되면서 사람들이 종이 달러를 다시 금으로 교환할 수 있게 되었습니다. 그러나 한 가지 문제가 있었습니다. 정부는 금의 환율을 온스당 35달러로 인상하면서 종이 달러 가치를 절하했습니다. 이로 인해 종이 달러의 가치가 하락하면서, 저소득층과 중산층의 재산 가치가 크게 감소하여 많은 사람들이 가정 경제에 타격을 입었습니다.

제2차 세계대전 이후 1944년 브레튼우즈 협정을 통해 미 달러가 세계 기축 통화로 지정되었으며, 금으로 교환할 수 있는 통화가 되었습니다. 그러나 1971년尼克 대통령이 미 달러의 금 태환을 종료하면서 미 달러와 금의 연결이 끊어졌습니다. 이것은 달러가 금과 같은 실물 자산에 으로 뒷받침되지 않고 사용자들 신뢰와 신용에 기반을 둔 명목화폐 체제로 전환되는 계기가 되었습니다. 한편 정부와 중앙은행이 대부분의 금을 보유하게 되면서 금의 가치는 급등하여 1980년에는 온스당 870달러에 이르렀습니다.

온스당 금의 가치



이 이야기는 건전화폐가 불건전화폐(명목화폐)로 전환되어 정부와 은행이 국민들에게 귀금속을 수탈한 방법을 보여줍니다. 실제 화폐는 정부와 은행의 손에 들어갔고, 사람들에게는 정부가 강제로 사용을 명령하는 종이 조각만 남겨졌습니다.

금과 다양한 통화의 금 기준 측정, 1900–2023



4.2 명목화폐 시스템

“

기존 화폐의 오래된 문제는 유지되기 위해 요구되는 신뢰입니다. 중앙은행이 화폐 가치를 떨어뜨리지 않을 것이라는 신뢰가 필요하지만, 명목화폐 역사는 그 신뢰를 저버린 사례들로 가득합니다.

사토시 나카모토

”

인류는 다수가 통제하는 건전화폐에서 소수가 통제하는 불건전화폐로 전환되었습니다. 하지만 이 시스템은 어떻게 작동할까요?

4.2.1 법령에 의한 화폐 시스템

명목화폐 시스템은 법으로 사용이 강제된 특성이 있으며, 법령을 통해 사람들이 사용하도록 강요 받습니다.

“Fiat”라는 단어는 라틴어에서 유래한 것으로, “법령으로” 라는 뜻이며 이는 정부나 권위 있는 기관이 내리는 명령을 의미합니다.

금과 같은 실물 자산으로 뒷받침되는 화폐와 달리, 명목화폐는 뒷받침 되는 것이 없지만 법으로 사용이 강제됩니다.

달러, 유로, 파운드, 위안, 폐소 등 우리가 일상에서 사용하는 화폐들은 모두 명목화폐에 해당합니다.



강제화 된 법령: 모든 국민이 특정한 형태의 화폐를 강제로 받아들이도록 하는 법률.

명목화폐 가치는 상품과 서비스로 교환될 수 있다는 믿음과, 시간이 지나도 가치를 유지할 것이라는 착각에 기반을 둡니다.

명목화폐는 마치 콘서트 티켓과 같습니다. 종이 티켓에 가치가 있는 것이 아니라, 밴드(정부와 중앙은행)가 좋은 공연(경제 안정)을 제공할 것이라는 보장에 가치가 있습니다.

명목화폐 장점

- 💡 **사용이 편리함:** 명목화폐는 일상 거래에 매우 편리합니다.
- 💡 **비용 절감 및 낮은 보안 위험:** 금과 달리 강한 보안이 필요하지 않으므로 보관 및 사용이 더 저렴하고 안전합니다.

명목화폐 단점

- 💡 **인플레이션 위험:** 가격이 끊임없이 상승하여 인플레이션이 발생할 수 있으며, 초인플레이션 사례도 존재합니다.
- 💡 **중앙 집중 통제 및 조작 가능성:** 일부 소수의 집단이 시스템을 조작하거나 검열 및 자산 몰수를 할 가능성이 있습니다.
- 💡 **신뢰 당사자 위험:** 정부가 경제 위기를 겪으면, 해당 화폐 가치가 급락할 수 있습니다.
- 💡 **악용 가능성:** 시스템이 부패하거나 신뢰를 잃게 될 경우, 경제 불안과 부정부패로 이어질 수 있습니다.

명목화폐란 무엇이며, 누가 통제하는가?

상품화폐 vs. 명목화폐: 차이를 떠올려 보세요

기억하세요: 정부는 명목화폐가 등장하기 전에 금이나 은처럼 귀하고 얻기 어려운 실물 자산으로 주화를 주조하거나, 실물 자산으로 교환할 수 있는 종이화폐를 발행했습니다. 이것이 상품 기반 화폐 시스템(commodity-backed system)이었습니다.

하지만 현재 명목시스템(fiat system)은 마치 “모노폴리 게임”的 돈과 비슷합니다. 명목화폐는 중앙은행이 인쇄한 종이에 불과하며, 그 가치는 정부 정책에 따라 영향을 받습니다. 정부와 중앙은행은 “모노폴리 게임의 은행”처럼 시스템을 운영하고 돈의 흐름을 결정하며 무엇이 가치가 있는지 통제합니다. 즉 정부는 자신들이 화폐 시스템을 잘 관리하겠다고 약속하는 것입니다.

그 결과, 명목화폐는 정부가 사용을 강제하기 때문에 가치가 있을 뿐이며 그 자체로는 아무런 가치가 없습니다.

명목화폐 시스템은 “신뢰”에 기반한 게임이며 돈의 가치는 정부 약속에 의존한다고 요약 할 수 있습니다. 국민들은 정부가 공익을 위해 행동할 것이라고 기대할 수밖에 없습니다. 다음 장에서는 은행이 새로운 돈을 만들어내는 방법, 누가 관여하는지, 그리고 경제에 어떤 영향을 미치는지 살펴보겠습니다.

4.2.2 은행 부분지급준비 제도: 부채로 운영되는 시스템

“

국민들이 우리의 은행 및 화폐 시스템을 이해하지 못하는 것이 차라리 다행이다.
만약 국민들이 이해한다면, 내일 아침이 되기 전에 혁명이 일어날 것이라고 확신한다.

핸리 포드

”

은행의 부분지급준비 제도(Fractional reserve banking)는 명목화폐 시스템 핵심 요소 중 하나로, 은행이 고객의 예금 중 상당 부분을 대출할 수 있도록 합니다. 은행들이 고객들에게 다양한 서비스를 제공하는 이유를 궁금해한 적이 있나요? 겉으로는 은행이 고객들에게 많은 서비스를 제공하는 것처럼 보일 수 있지만 은행도 이윤을 추구하는 기업이라는 점을 기억해야 합니다. 그렇다면 은행은 돈을 빌려주면서도 어떻게 수익을 창출할 수 있을까요? 은행들은 어디에서 돈을 빌려올까요?

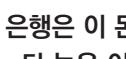
은행은 다음과 같은 방법으로도 수익을 창출합니다:

- ✿ 대출 이자를 부과
- ✿ ATM 이용료 및 계좌 유지 수수료와 같은 서비스 요금 부과
- ✿ 증권 매매나 부동산 투자 등 다양한 투자 활동을 통해 수익 창출
- ✿ 대출 금액 일부를 준비금으로 보유하고 나머지를 투자하거나 재대출
- ✿ 예금 이자를 지급하면서도 당좌 및 저축 계좌에서 수수료 부과

은행은 고객에게 예금을 받으면, 일정 비율(지급준비율)만 유지하면 되고 나머지 금액은 대출을 해줄 수 있습니다



은행은 예치자한테 낮은 이율로
돈을 빌립니다.
(이율 5%)



은행은 이 돈으로 채무자에게
더 높은 이율로 대출해줍니다.
(이율 9%)



은행은 대출을 통해 받은 이자
(9% - 5% = 4%)에서
예치자에게 이자를 지급하고,
나머지를 이윤으로 남깁니다.



제 4장



예를 들어 지급준비율이 10%일 때, \$100을 예치하면 은행은 \$10만 준비금으로 보유하고 \$90를 대출해줄 수 있습니다. 대출받은 사람이 \$90을 또 다른 은행에 예치하고 반복하면 결국 초기 \$100 예금이 점점 늘어나면서 총 통화량은 \$271로 증가합니다. 이는 마치 돈이 마법처럼 창조되는 것처럼 보이는 현상이며 승수 효과(multiplier effect)라고 합니다.

이 과정은 부채 중심의 화폐 시스템으로 이어지며, 은행은 대출을 통해 새로운 통화를 창출하여 전체 통화 공급을 증가시킵니다. 은행 부분지급준비 제도가 지속됨에 따라, 우리경제의 총 부채가 증가하며 인플레이션을 유발합니다.

이 시스템은 대출을 통한 끊임없는 화폐 창출에 의존하는데 마치 마약 중독자가 계속 마약을 먹는 것과 유사합니다. 하지만 은행이 보유한 준비금보다 많은 돈을 대출해주는데, 예치자들이 동시에 예금을 인출하면 은행은 파산합니다.

이때 중앙은행이 최후의 대부자(lender of last resort)로 개입하여, 새로운 통화를 공급함으로써 은행 붕괴를 막습니다. 중앙은행은 자산을 다시 매입하거나 은행 계좌에 직접 통화를 주입하는 방식으로 수행합니다.

결국 중앙은행이 계속 새로운 통화를 투입하여 은행을 구제하는 이 부채 기반 시스템은 경기 호황과 불황을 반복하는 결과를 초래합니다

여러분에게 세일러라는 은행원 친구가 있다고 가정해 보세요.

세일러는 여러 곳을 다녀야 해서 자전거를 빌리고 싶어 합니다. 여러분은 흔쾌히 자전거를 빌려주지만, 알고 보니 세일러는 여러분에게 빌린 자전거를 친구들에게 모두 빌려주겠다고 약속합니다. 즉 세일러는 여러분이 빌려준 단 한 대의 자전거를 가지고 여러 대의 “상상 속 자전거”를 만들어내며 친구들에게 빌려주기 시작합니다. 세일러 친구들은 언제든지 자전거를 이용할 수 있다고 믿지만 실제 자전거는 오직 한 대 뿐이고, 나머지는 모두 “상상 속 자전거”라는 게 문제입니다.

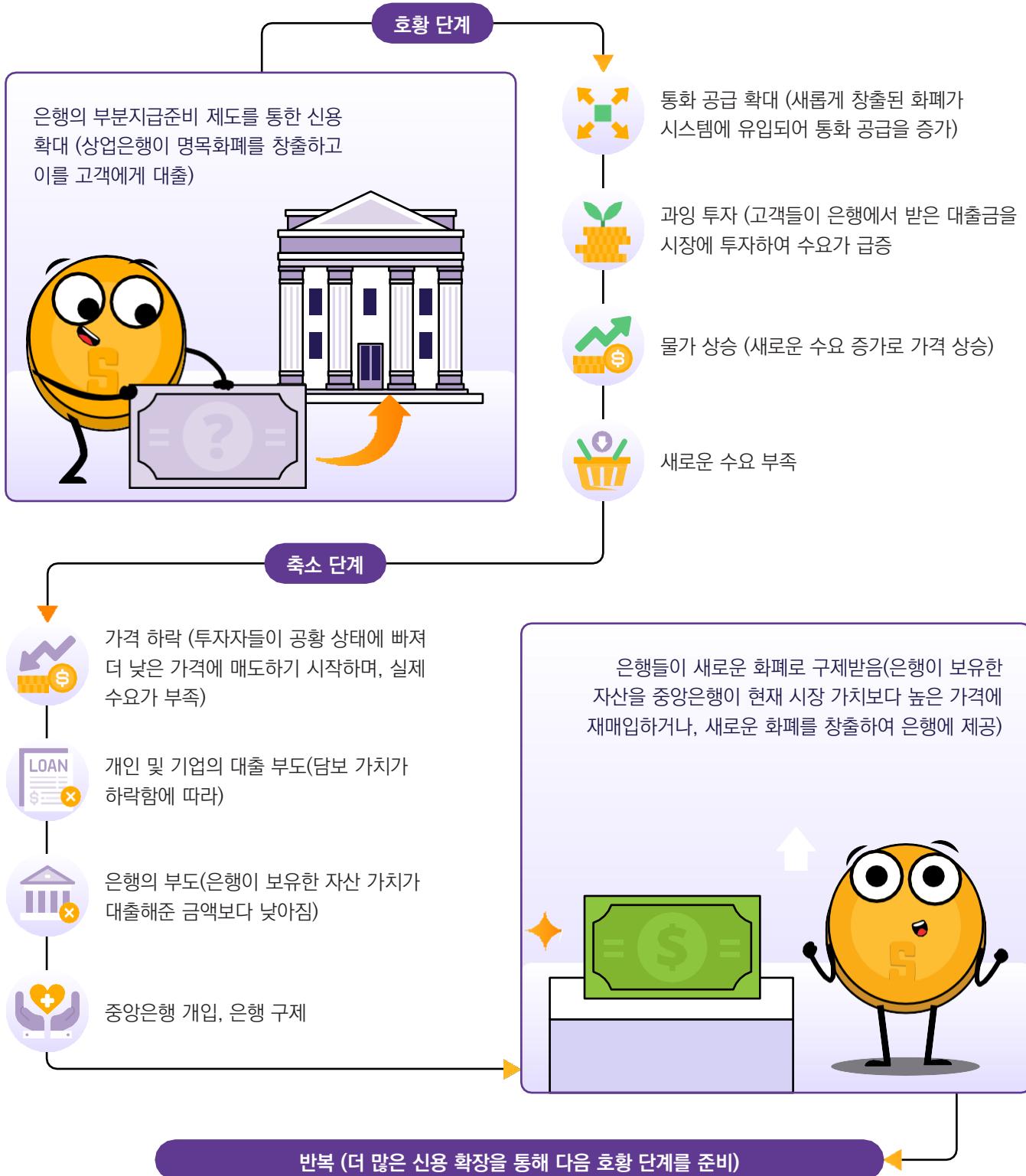
그렇다면 어떻게 될까요? 상상 속 자전거를 사용 할 수 있다는 약속에 모두가 행복해 합니다. 왜냐하면 처음에는 자전거를 모두가 동시에 사용하지 않기 때문에 문제가 없어 보입니다. 마치 자전거가 넘쳐나는 것처럼 느껴지고, 친구들은 자전거를 타고 갈 곳들을 계획하며 들떠 있습니다.

하지만 이 마법이 깨지는 순간이 옵니다. 날씨 좋은 어느 날 모든 친구들이 동시에 자전거를 타기 좋은 날이라고 생각하고 다들 세일러의 집으로 달려가 자전거를 빌리려 합니다. 그러나 이제 현실이 드러납니다. 실제로 존재하는 자전거는 단 한 대 뿐이기에 친구들은 당황하고 실망하며 모두가 기대했던 자전거의 가치가 한순간에 사라집니다.

부분지급준비대출 세계에서도 똑같은 일이 벌어집니다. 은행들은 실제 돈보다 더 많은 돈을 대출해주며, 처음에는 모두가 그 혜택을 누리는 것처럼 보입니다. 돈이 더 많이 유통되고 경제가 풍요로워진 듯 보입니다. 하지만 많은 사람들이 동시에 예금을 인출하려 한다면 상황이 달라지며, 그때서야 비로소 실제 가치가 드러납니다. 모든 약속을 이행할 만큼 충분한 돈이 존재하지 않는다는 사실이 밝혀지는 것입니다.

이러한 상황은 사회에 심각한 영향을 미치고 모든 사람들의 화폐 가치를 떨어뜨립니다. 넘쳐나는 것처럼 보였던 돈은 결국 사기가 됩니다. 마치 친구들 모두 동시에 자전거를 타려고 할 때 자전거 가치가 사라지는 것처럼, 사람들이 동시에 돈을 찾으려 하면 화폐 가치가 급락하게 됩니다. 결국 사람들은 자신이 은행에 맡겨둔 돈이 실제로 존재하지 않는다는 사실을 깨닫게 됩니다. 이것이 “뱅크런”을 초래하고, 경제 전체의 붕괴로 이어지는 과정입니다. 그리고 피해를 가장 많이 보는 계층은 항상 동일했습니다. 바로 전세계 저소득층과 중산층입니다.

명목화폐란 무엇이며, 누가 통제하는가?



제 4장



체험 활동: 은행의 부분지급준비 제도

우리는 은행 부분지급준비 제도가 화폐 가치의 저하, 인플레이션, 그리고 구매력 감소로 이어질 수 있는지 탐구해볼 것입니다. 6명의 참여자로 진행하며, 그중 한 명은 은행 역할을 맡게 됩니다. 그리고 오늘날 지급준비율인 10%를 적용할 것입니다.

- ◆ A가 복권에서 \$100,000에 당첨되었고 B은행에 예금합니다. 지급준비율이 10%이므로 B은행은 \$10,000을 금고에 보관해야 하며, 나머지 \$90,000을 대출해 줄 수 있습니다.
- ◆ C가 최대 금액(\$90,000)을 B은행에서 대출받아 D의 집을 구매하는 데 사용합니다.
- ◆ D는 C로부터 받은 \$90,000을 B은행에 예금합니다. 그리고 B 은행의 총 예금액은 \$190,000이 됩니다.
- ◆ E가 B은행에 대출을 요청하며, 은행은 새로운 예금(\$90,000)의 90%인 \$81,000을 대출해줍니다.
- ◆ E는 \$81,000 대출금으로 F의 예술 작품을 구매합니다. 이후 F는 돈을 다시 B 은행에 예금합니다. B은행 총 예금액은 이제 \$271,000이 됩니다.

체험 활동 결과 처음 \$100,000 예금이 경제를 순환한 후 총 \$271,000 통화가 만들어졌습니다.

만약 지급준비율이 1%로 낮아진다면, 생성되는 화폐의 양은 훨씬 더 많아질 것입니다.

$$\$100,000 \div 0.01 = \$10,000,000.$$

\$100,000가 경제를 계속 순환한다면 실제로 얼마나 많은 화폐가 창출될까요?

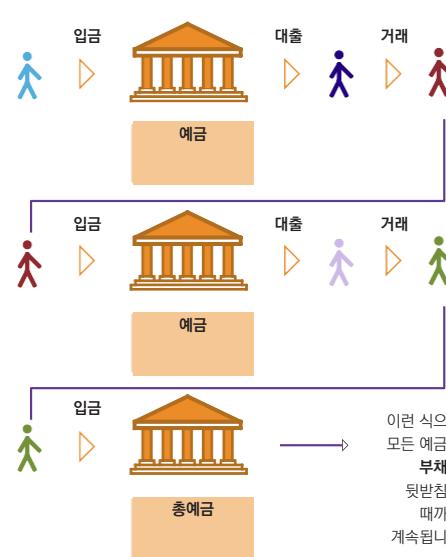
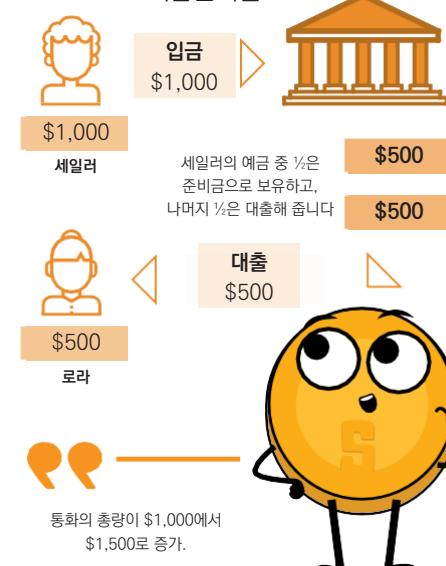
여기서 중요한 점은 2020년부터 미국 연방준비제도가 경제를 활성화 하려고 지급준비율을 0%로 낮췄다는 것입니다.

6명의 참여자 역할입니다:

- A = 예금자 (복권 당첨자) (연한 파랑)
- B = 은행원 (은행)
- C = 채무자 #1 (짙은 파랑)
- D = 부동산 소유자/예금자 (빨강)
- E = 채무자 #2 (연한 보라)
- F = 미술관 소유자/예금자 (초록)

은행의 부분지급준비 제도

지급준비율 50%



명목화폐란 무엇이며, 누가 통제하는가?

4.2.3 누가 명목화폐 시스템을 통제하며, 이익을 얻는 방법은 무엇인가?

명목화폐 시스템을 통제하는 주체는 네 가지입니다: 정부, 정치인, 금융권, 그리고 중앙은행.

정부: 정부는 마치 명목화폐 시스템라는 쇼의 감독과 같습니다. 세금을 걷는 것 외에도 재무부가 발행하는 새로운 부채(채권)를 통해 자금을 조달합니다. 만약 채권 수요가 충분하지 않아 채권이 남으면 중앙은행이 매입합니다.

이로 인해 정부는 국민 승인을 받을 필요 없이 이익을 추구할 수 있습니다. 마치 신용카드를 사용하면서 카드 값에 대해 전혀 걱정하지 않는 것과 같습니다. 이런 방식은 정부에는 유리해 보일 수 있지만, 그 대가는 결국 모든 국민들에게 전가됩니다.

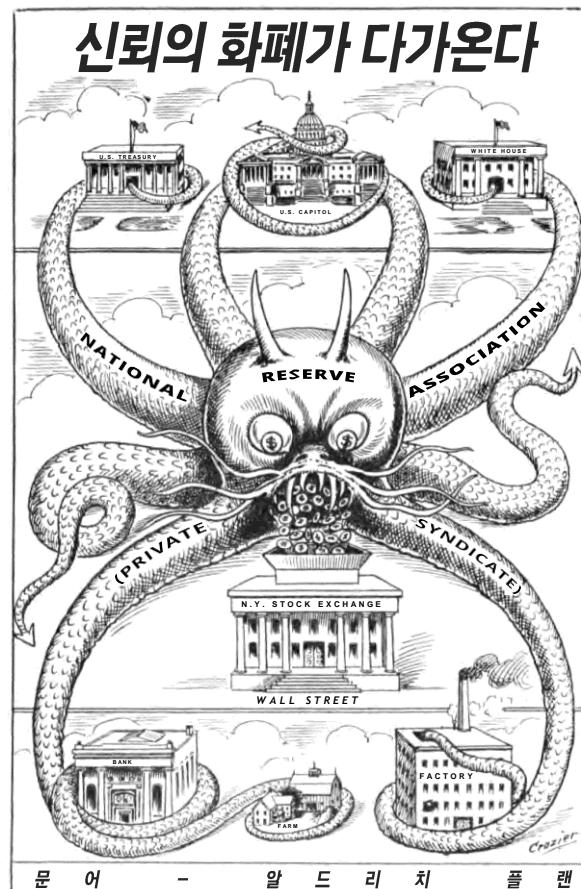
정치인: 정치인들은 명목화폐 시스템에서 많은 이익을 얻습니다. 더 많은 부채를 축적할 수 있는 능력을 바탕으로, 원자재, 부동산, 주식과 같은 자산에 투자하여 매우 적은 노력으로 새로운 부를 창출할 수 있습니다.

금융권(은행): 은행과 기타 금융 기관들은 명목화폐 시스템을 직접 통제하지는 않지만, 막대한 이익을 얻습니다. 부분지급준비대출을 통해 새로운 화폐를 창출하는 과정을 가속화할 수 있으며 더 높은 수익을 창출할 수 있습니다. 그리고 사실상 은행들은 결과에 대한 책임도 지지 않습니다, 왜냐하면 시스템 붕괴를 막으려고 중앙은행이 새로운 명목화폐를 발행하여 구제해주기 때문입니다.

중앙은행: 중앙은행은 명목화폐 시스템을 조종하는 기관으로, 통화량 공급을 통제하는 역할을 맡고 있습니다. 하지만 여기에는 속임수가 있는데, 중앙은행 또한 정부의 법에 따라 움직이며 정부 이익을 지키려고 존재합니다. 즉 꼭두각시 인형사가 또 다른 꼭두각시 인형사에게 조종당하는 것과 같습니다. 중앙은행이 시스템을 통제하는 것처럼 보일 수 있지만 사실 정부가 필요할 때마다 무에서 돈을 창출할 수 있도록 돋는 역할을 합니다.

이 주체들은 다양한 방식으로 이익을 얻으며, 복잡한 통제 구조를 형성합니다. 정부는 편하게 자금을 조달할 수 있으며 정치인과 은행은 아무런 노력 없이 돈을 벌어들일 수 있고 중앙은행은 시스템이 유지되도록 합니다. 한편, 대다수 국민들은 명목화폐 시스템 때문에 점점 더 큰 어려움을 겪게 됩니다.

결국 명목화폐 시스템의 조종자들은 소수에게는 엄청난 이익을 안겨주지만 대다수 사람들은 자신이 속한 금융 시스템이 과연 공정한지 고민할 수밖에 없는 현실을 마주하게 됩니다.



중앙은행 역할

중앙은행은 조용히 경제가 작동하는 방식을 결정합니다. 중앙은행의 역할은 신뢰성을 유지하고 경제를 안정하게 운영하는 것이지만, 그 방식에는 더 비밀스러운 것이 숨어 있습니다.

중앙은행은 정부와 긴밀하게 협력하며 통화정책을 조종하고 금리와 같은 도구를 사용하여 통화 공급을 통제합니다. 위기가 발생하면 무에서 돈을 창조하여 상업은행을 통해 경제에 투입하여 모든 것이 정상으로 보이게 만듭니다.

하지만 단순히 경제를 감시하는 것에 그치지 않습니다. 중앙은행은 상업은행을 규제하고 금융 시스템 규칙을 설정하며, 은행이 위기에 처하면 “최후의 대부자(lender of last resort)” 역할을 수행합니다. 이러한 거미줄 같은 통제 시스템은 겉으로 보기에는 경제를 보호하는 것처럼 보이지만, 결국 경제와 상업은행을 중앙은행에 더욱 의존하게 만드는 결과를 초래합니다.

수조 달러 규모의 경기 부양 자금이 어디에서 나오는지, 누가 그 자금을 배분하는 결정을 내리는지 이해하는 것은 더 넓은 금융 시스템을 파악하는 데 필수입니다. 정부는 특정 시점에서 통화 공급을 관리하려고 여러 도구를 사용합니다.

중앙은행과 정부는 통화정책(Monetary Policy)과 재정정책(Fiscal Policy)을 활용하여 통화 공급과 경제에 영향을 미칠 수 있습니다. 예를 들어 미국 연방준비제도(Federal Reserve, Fed)는 통화정책을 통해 금리를 조정하며 경제 내 유통되는 화폐량에 직접 영향을 줍니다. 반면 재정정책은 정부 지출 및 세금 정책을 활용하여 경제 활동에 영향을 미칩니다.

목표 금리 통화정책

실업률
6.5% 이하



연간 국내총생산
(GDP)
2% ~ 3% 증가



근원
인플레이션
2.0%~2.5% 사이

재정정책 확장

소비 지출과 기업 투자를
증가시켜 총수요와 경제 성장을
촉진하는 것을 목표로 합니다.



정부
지출 증가

VS

재정정책 긴축

소비 지출과 기업 투자를 줄여
지속 불가능한 경제 성장을
둔화시키고, 높은 인플레이션을
방지하거나 감소시키는 것을
목표로 합니다.



세금
증대

명목화폐란 무엇이며, 누가 통제하는가?

환율 정책, 공급 충격, 그리고 가격 통제로 통화 공급을 조절하고 무역 및 경제에 영향을 미칩니다. 이러한 정책은 물가 안정과 인플레이션 통제를 목표로 하지만, 중앙은행 개입이 이루어질 경우 경기의 호황과 불황이 반복되는 사이클을 초래하며 모든 사람들에게 어려움을 야기할 수 있습니다.

예시: “대마불사(Too Big to Fail)”란 규모가 너무 크고 서로 연결되어 있어, 만약 파산할 경우 금융 시스템 전체에 큰 영향을 미칠 수 있는 금융 기관을 의미합니다. 2008년 금융위기 당시 여러 대형 은행들이 대마불사로 간주되어 미국 정부가 이들의 붕괴를 막으려고 구제 금융을 했습니다.

2008년 금융위기에서 가장 잘 알려진 대마불사 사례 중 하나가 바로 투자은행 리먼 브라더스(Lehman Brothers)였습니다. 리먼 브라더스는 2008년 9월 파산을 신청했으며 연쇄 충격을 야기했습니다. 그 결과 보험 대기업 AIG가 파산 직전까지 몰렸으며, 주식 시장이 급락했습니다. 결국 미국 정부는 다른 주요 금융 기관들에 구제 금융을 제공함으로써 혼란을 방지하고 금융시스템을 보호하려 했습니다.

이러한 정책이 작동하는 방법을 이해하는 것은 중앙집중식 명목화폐 시스템 한계를 파악하는 데 필수입니다. 문제를 이해해야만 해결책을 찾을 수 있기 때문입니다. 이제까지 과거와 현재의 명목화폐 시스템이 운영되어 온 역사를 살펴보았으므로, 이제 명목화폐 미래인 중앙은행 디지털 화폐(CBDC)에 대해 이야기해 보겠습니다.

4.3 중앙은행 디지털 화폐(CBDC): 명목화폐의 미래

중앙은행 디지털 화폐(CBDC)는 명목화폐 다음 단계입니다. 기존의 명목화폐가 지폐, 동전, 그리고 디지털 결제를 포함하는 형태라면, CBDC는 정부가 발행하고 중앙은행이 통제하는 완전한 디지털 형태의 화폐입니다.

우리가 일상에서 사용하는 화폐를 상상해 보세요. 주머니 속에서 달그락거리는 동전도, 접어 보관하는 지폐도 없습니다. CBDC의 가장 큰 특징은 정부와 중앙은행이 금융 거래를 보다 정밀하게 감시하고 통제할 수 있다는 점입니다. CBDC를 통해 정부는 돈의 흐름을 추적하고 규제하는 것이 훨씬 쉬워집니다.

정부와 중앙은행은 CBDC의 형태와 발행량을 조정할 수 있으며, 금리를 조작하고 보다 정밀한 통화 및 재정 정책을 실행할 수 있습니다. 즉 CBDC는 정부가 명목화폐를 관리하고 영향을 미치는 더 빠른 수단을 제공합니다.

CBDC가 명목화폐의 미래로 보이지만, 현재 세계 통화 시스템은 이미 명목화폐 표준(fiat standard)에 기반하고 있습니다. 오늘날의 명목화폐는 금과 연결되지 않으며 제한 없이 통화 공급이 크게 확대되었습니다.

이제 명목화폐 시스템이 작동하는 원리를 더 명확히 이해했으므로, 다음 장에서는 이러한 시스템이 초래하는 결과를 살펴보겠습니다.

제 5장

문제를 어떻게 해결해야 하는가?

5.0 서론: 문제

5.1 구매력 감소

5.1.1 화폐 인플레이션과 구매력에 미치는 영향

체험 활동: 인플레이션 효과 – 경매

5.2 전 세계 부채 부담과 사회 불평등

5.2.1 개인에 미치는 영향 – 구매력 손실

5.2.2 사회에 미치는 영향 – 부의 불평등 증가

체험 활동: 명목화폐 시스템의 결과

5.2.3 전 세계의 부채 부담

5.3 사이퍼펑크와 분산형 화폐가 걸어온 길

5.3.1 사이퍼펑크

5.3.2 중앙화 시스템 vs 분산화 시스템

5.3.3 디지털 화폐의 간략한 역사

학습 워크북

한국어 버전 | 2025

문제를 어떻게 해결해야 하는가?

5.0 서론: 문제

“

통화량을 통제하는 자는 모든 산업과 상업을 완전히 지배하는 자입니다.
소수의 강력한 인물들이 모든 시스템을 매우 쉽게 통제하고 있다는 것을 깨닫는다면,
인플레이션과 경기침체가 시작되는 설명을 들을 필요도 없을 것입니다.

제임스 A. 가필드, 미국 대통령

”

4장에서 기존 금융시스템이 생각만큼 튼튼하지 않을 수도 있다는 사실을 배웠습니다. 무한히 발행되는 종이돈으로 유지되는 명목화폐 시스템은 소수에게만 더 큰 혜택을 제공하며 다수의 구매력은 하락합니다. 이번 장에서는 명목화폐 시스템이 일반 사람들과 사회에 어떤 의미를 가지는지를 살펴봅니다. 마지막으로 이러한 문제를 알아차리고 인류 사회가 갈 미래를 변화시킬 해결책을 조용히 찾아낸 어느 그룹 이야기를 탐구해 보겠습니다.

5.1 구매력 감소

5.1.1 화폐 인플레이션과 구매력에 미치는 영향

통화 인플레이션은 통화 공급이 증가하는 현상을 말하며, 사람들 구매력을 줄어들게 만듭니다. 인플레이션 순환은 유통되는 돈이 많아지면서 시작되며 상품과 서비스의 수요를 증가시키며 가격 상승을 초래합니다.

트럼프, 세일러, 로라라는 세 명의 친구가 있다고 가정해 봅시다. 각자 1달러가 있으며 판매 중인 물병은 단 한 병 뿐입니다. 이제 지방정부가 친구들에게 각각 1달러씩 추가로 지급했다고 가정해 보겠습니다. 세 사람은 이제 총 6달러를 소유합니다. 친구들은 돈이 많아졌기 때문에 모두 그 물병을 사고 싶어 합니다. 모든 친구들이 같은 물병을 원하기 때문에 서로 경쟁하며 가격을 제시하기 시작합니다.

이 추가된 돈이 일으킨 수요 증가는 결국 물병 가격을 상승시킵니다. 결국 친구들은 더 높은 가격을 지불하게 되어 구매력이 감소합니다. 이전보다 더 많은 돈이 있지만 더 적은 양이 되어 버린 물병만 구매할 수 있게 됩니다. 이는 인플레이션이 돈 가치에 미치는 영향을 보여주는 예입니다.

친구들 통화는 정부가 발행한 통화량에 영향을 받아 구매력이 감소했습니다. 제한없는 통화 공급과 물건 구매 수요 증가가 결합되어 가격 상승으로 이어졌습니다. 그 결과, 친구들은 더 많은 달러로도 같은 크기 물건을 구매하기 어려워졌습니다.

이 상황은 친구들 구매력이 그들이 통제할 수 없는 요인으로 영향을 받았음을 보여줍니다. 우리 돈 가치에 영향을 주는 시스템을 이해하고, 의문을 던지는 일이 중요함을 강조합니다.

이제 이러한 상황이 현실에서 나타나는 현상을 탐구해 보겠습니다.



제 5장

체험 활동: 인플레이션 효과 - 경매

목표: 인플레이션 개념과 그것이 경제에서 상품과 서비스의 가격에 어떤 영향을 미치는지 이해하기.

정의

 통화 공급: 특정 시점에서 경제 내 유통되고 있는 총 통화량으로 다음이 포함됩니다:

- 실물 화폐 (주화 및 지폐)
- 예금 계좌
- 저축 예금
- 머니마켓 계좌(Money Market Accounts)
- 소액 정기 예금: \$100,000 미만의 예금증서 (Certificate of Deposit)

 경매: 상품이나 재산이 최고 입찰자에게 판매되는 공개 판매 방식.

수업 활동 — 아래 지시사항을 따르세요:

1. 선생님으로부터 무작위로 모노폴리 돈을 받습니다. 이는 통화 공급을 나타냅니다.
2. 제공된 표에 총 통화 공급을 적으세요.
3. 선생님이 학생들을 대상으로 캔디바를 경매에 부칩니다. 캔디바를 얻으려면 모노폴리 돈을 사용해 가장 높은 입찰가를 제시해야 합니다. 최고 입찰가를 통화 공급 옆에 기록하세요.
4. 선생님이 모노폴리 돈을 대량으로 추가합니다. 이는 경제 내 통화 공급 증가를 나타냅니다. 나중에 경제에서 통화 공급이 증가하거나 감소하는 원리를 배우게 될 것입니다.



사회는 종종 예측할 수 없고 불공정할 수 있습니다. 마치 선생님이 무작위로 소수 학생들에게만 많은 돈을 주는 시뮬레이션으로 설명할 수 있습니다. 이 예시는 현실에서의 자원과 기회의 분배가 불공정하게 이루어지는 상황을 보여주며, 더 나아가 내재된 무작위성과 불공정성을 부각시킵니다.

5. 선생님이 두 번째 캔디바를 같은 방식으로 학생들에게 경매에 부칩니다.
6. 표에 통화 공급 옆에 최고 입찰가를 기록하세요. 그리고 선생님은 세 번째 경매도 반복할 것입니다."

문제를 어떻게 해결해야 하는가?

라운드	통화 공급	최고 입찰가
1		
2		
3		

결론:

1. 통화 공급 증가가 캔디바의 최고 입찰가에 어떤 영향을 미쳤나요?
2. 통화 공급 증가와 인플레이션 간 관계는 무엇인가요?
3. 통화 공급이 실제 세계에서 어떤 관련성이 있나요?
4. 경제에 새로운 돈이 투입되면, 상품과 서비스의 가격에 어떤 일이 생길 것이라고 생각하나요? 가격 변동이 지금의 문제일까요, 아니면 영원히 일어날까요? 왜 그렇게 생각하나요? 가격 변화가 오랜 기간에 걸쳐 사람들에게 어떤 영향을 미칠 것이라고 생각하나요?

5.2 전 세계 부채 부담과 사회 불평등

5.2.1 사회에 미치는 영향 – 구매력 상실

세일러는 소형 아파트에서 거주하는 대학생입니다. 그는 생활비와 학비를 충당하려고 커피숍에서 파트타임으로 일합니다. 독립하자마자 장부를 잘 관리하는 법을 익혔습니다.



장부란 모든 금전 거래를 자세히 기록한 문서를 말합니다.
돈을 벌거나 쓴 모든 것을 관리하고 추적하는 데 도움을 줍니다.

그는 2023년 초에 1년 생활비 예산을 \$10,000로 잡았습니다. 여기에는 월세, 식비, 기타 생필품이 포함되었습니다.
다음은 2023년 1월 동안 그의 거래 내역입니다:

제 5장

날짜	사용처	금액	유형	잔액
2023년 1월 1일	생활비 예산	\$1,600		\$1,600
2023년 1월 1일	1월 월세	\$800	차감	\$800
2023년 1월 5일	식료품비	\$100	차감	\$700
2023년 1월 15일	파트타임 급여	\$500	추가	\$1,200
2023년 1월 20일	자동차 기름값	\$350	차감	\$850
2023년 1월 30일	교재비	\$150	차감	\$700

장부는 세일러의 생활비 예산이 \$1,600이었음을 보여줍니다. 그 중 \$800을 월세로 지출했습니다. 이후 \$100을 식료품비로 사용했으며, 파트타임 급여로 \$500를 받으면서 잔액이 \$1,200이 되었습니다. 이후 그는 자동차 기름값과 교재비로 돈을 지출하여 이달 말 잔액은 \$700이 되었습니다.

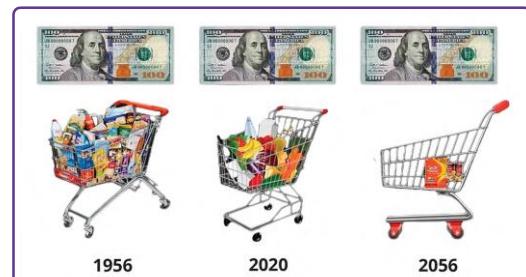
1년 후 세일러는 할아버지와 점심을 먹으며 내년 생활비 예산에 대해 이야기를 나눕니다. 세일러는 예산이 이전만큼 충분하지 않으며, 지난 1년 동안 생활비가 크게 증가했음을 깨닫습니다. 왜 이런 일이 일어났는지 궁금해하던 중 할아버지가 다음 이미지를 보여줍니다.

세일러는 믿을 수 없었습니다. 왜냐하면 시간이 지나면서 상품과 서비스 비용이 급격히 증가하여 구매력이 감소한다는 사실을 깨닫았기 때문입니다.

할아버지가 말씀하셨습니다: “1956년에 나는 세상에 첫발을 내딛는 젊은이었습니다. 당시 공장 노동자로 일하며 한 달에 \$380을 벌었는데, 많아 보이지 않을 수도 있지만 당시에는 꽤 괜찮은 임금이었습니다. 사실 그 돈을 모아 교외에 집 한 채를 살 정도였습니다.”

할아버지는 계속해서 말씀하셨습니다: “지난 세월동안 물건 가격은 매년 달랐습니다. 예를 들어 2020년에 허쉬 초콜릿 바 30개를 사려면 \$26.14이 필요했지만, 1913년에는 같은 허쉬 초콜릿 바 30개의 가격이 단 \$1.00밖에 되지 않았습니다.”

이러한 큰 가격 차이는 구매력이 시간이 지나면서 어떻게 변했는지, 인플레이션 때문에 구매력이 얼마나 달라졌는지를 보여줍니다.

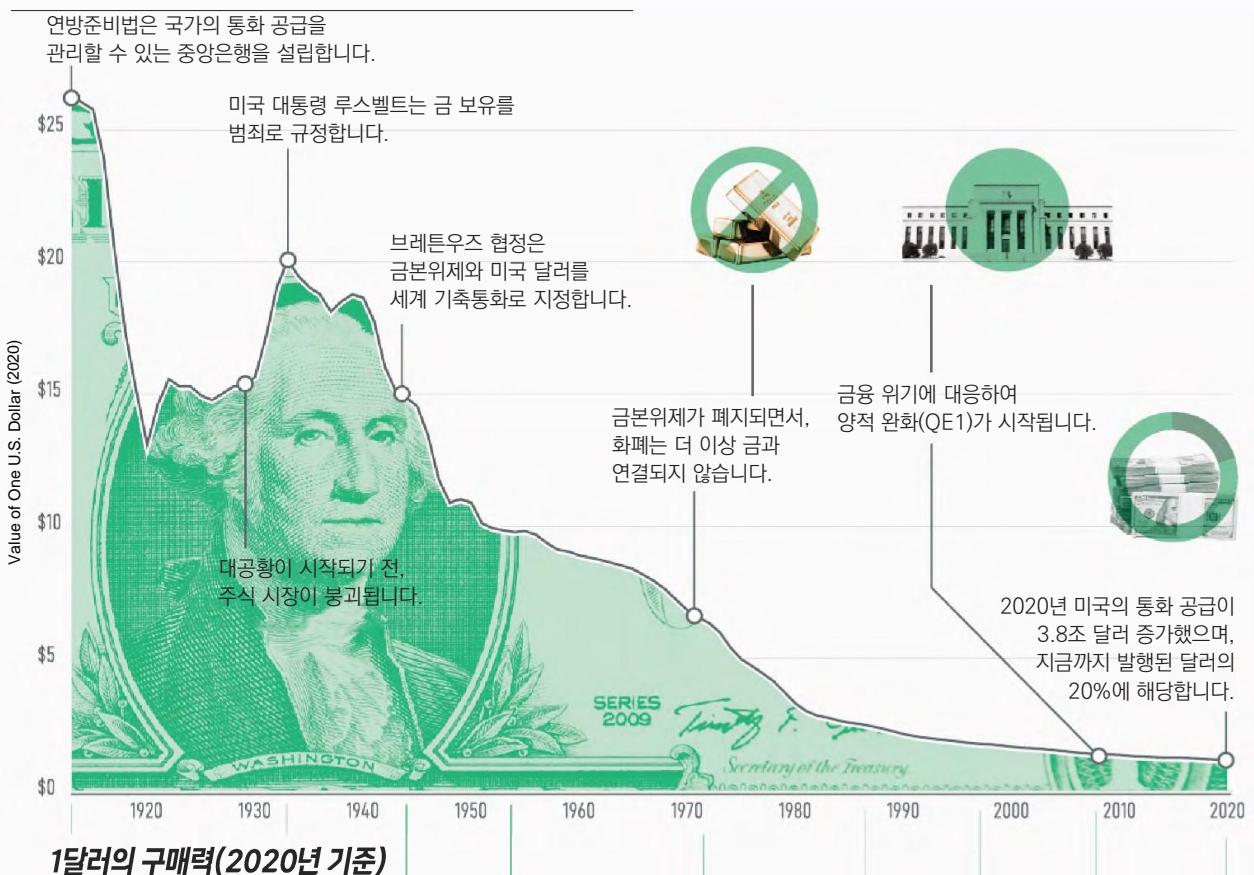


문제를 어떻게 해결해야 하는가?

달러의 가치

미국 달러의 구매력

지난 한 세기 동안 인플레이션과 통화 공급 증가로 인해
미국 달러의 구매력은 급격히 감소했습니다.



\$26.14	\$15.14	\$15.14	\$14.71	\$9.69	\$9.39	\$2.28	\$1.61	\$1.20	\$1.00
허쉬 초콜릿 바 30개	화장지 10롤	맥주 10병	코카콜라 10병	프리\레저 10봉지	오렌지 17개	크레용 2박스	자동 4개	레몬 2개	맥도날드커피 1잔
1913	1929	1933	1944	1953	1971	1987	1997	2008	2020

제 5장



세일러: “뭐라고요? 그게 말이 돼요. 그때 내 월세가 지금과 비교하면 얼마나 낮았을지 상상이 안 가요.”

할아버지: “그렇지, 그때는 월세가 훨씬 더 싼단다. 또 다른 예를 들어줄게. 그 당시에는 \$1로 프레첼 10봉지를 살 수 있었단다. 그런데 2020년에는 같은 양을 사는 데 \$9.69를 지불했어. 오늘날 프레첼 10봉지가 얼마나 비쌀지 한번 상상해 보렴.”

세일러: “와, 정말 흥미롭네요, 할아버지. 젊으셨을 때 이런 변화를 경험하셨나요?”

할아버지: “내가 젊었을 때는 모든 것이 훨씬 더 저렴했단다. 빵 한 덩이는 단 \$0.18밖에 안 했고, 휘발유 1갤런은 단 \$0.29였지. 생활비가 이렇게까지 많이 오른 게 정말 믿기지 않구나.”

할아버지와 대화를 마친 세일러는 집으로 돌아가 자신의 장부를 다시 살펴봅니다. 그는 올해 구매했던 동일한 상품과 서비스를 내년에 구매하기 위해서는 추가로 \$1,000 예산이 필요하다는 사실을 깨닫습니다. 이것은 그의 구매력이 \$1,000 감소했음을 의미합니다. 이제는 같은 상품과 서비스를 구매하려면 더 많은 돈을 지출해야 하기 때문입니다. 하지만 세일러의 급여는 조금 오르지만 필요한 생활비는 매년 급등하고 있습니다.

다음 표는 세일러의 첫해와 두 번째 해의 비용을 보여주며, 상품의 가격 상승률도 포함되어 있습니다.

세일러가 동일한 생활 수준을 유지하려면 더 많은 시간을 일해서 \$1,000을 벌어야 할 것입니다.

미국 노동통계국(US Bureau of Labor Statistics) 정보에 따르면 현재 물가는 1913년에 비해 약 30배 더 높습니다. 즉 오늘날의 1달러는 1913년의 1달러로 구매할 수 있었던 상품의 약 3%만 구매할 수 있다는 뜻입니다

종류	첫 해 비용	두 번째 해 비용	증가율 %
렌트	\$4,000	\$4,500	12.5%
식료품	\$2,000	\$2,300	15%
필수품	\$4,000	\$4,200	5%
합계	\$10,000	\$11,000	10%

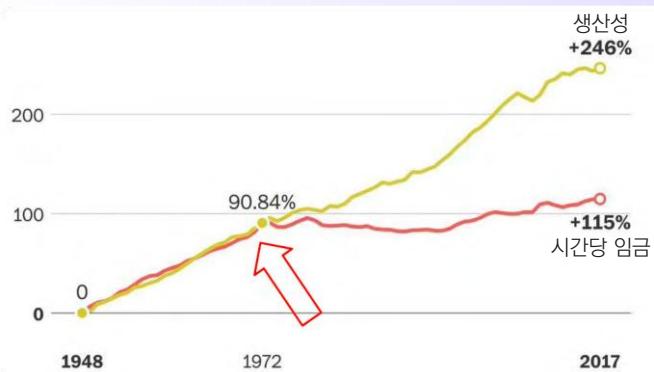
예를 들어 누군가 세일러에게 1913년에 \$100을 받거나 2023년까지 기다려 \$30,000를 받는 것 중 하나를 선택하라고 한다면 과거의 풍족한 쇼핑과 오늘날 몇 가지 작은 간식을 얻는 것 중에 선택하는 것과 같습니다. 이처럼 가치의 큰 차이는 세월이 지나면서 화폐의 구매력이 얼마나 감소했는지를 보여줍니다.

1938년 생활비	
생필품	
새 집	\$3,900.00
평균 연봉	\$1,731.00
새 차	\$860.00
평균 월세	\$27.00
하버드대학교 1년 학비	\$420
영화 티켓	¢25
주유비	갤런당 ¢10
우표	¢3
음식	
설탕	¢59
비타민 D 강화우유	¢50
드립 커피	¢39
베이컨	¢32
계란	¢18

문제를 어떻게 해결해야 하는가?

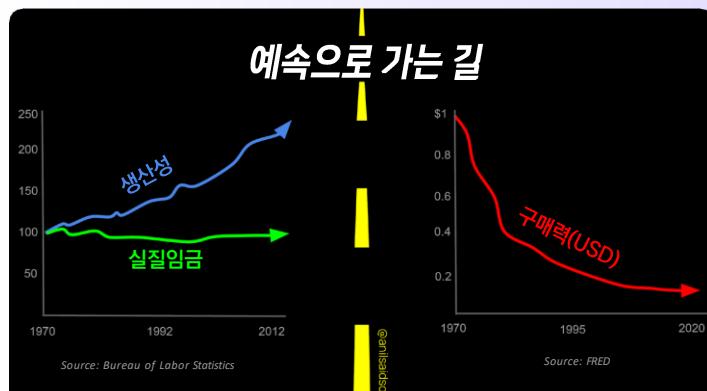
세일러는 명목화폐 숫자상 1년 동안 그의 할아버지가 벌었던 것보다 훨씬 더 많은 돈을 범니다. 하지만 할아버지가 가졌던 달러 구매력이 훨씬 더 가치가 있었고 더 많은 것을 살 수 있었습니다.

생산성 및 시간당 임금 성장률
(1948년 ~ 2017년)



참고: 급여에 생산 및 비관리직 근로자의 임금과 복리후생비 포함.

세일러의 예시는 많은 사례 중 하나일 뿐입니다. 명목화폐 세계에서는 정부가 목적을 달성하려고 무(無)에서 돈을 창조하는 일이 흔히 발생하며, 그로 인한 결과는 전 세계 사람들이 감당하게 됩니다. 빵에서 주택, 식료품에서 휴가비용까지, 모든 물품의 가격은 매년 상승합니다. 부자들은 자산을 보유하고 있기 때문에 인플레이션을 방어하지만, 그렇지 못한 사람들은 자신들이 힘들게 번 돈의 가치가 하락하는 것을 경험합니다. 그 결과, 전 세계 사람들과 가족들은 구매력이 감소하면서 어려움을 겪게 됩니다.



오늘날 심각한 인플레이션 때문에 사람들이 돈을 저축하는 것을 꺼리게 됩니다.

대부분 사람들은 돈의 가치가 빠르게 하락하기 때문에 즉시 소비하는 것을 선택합니다. 이러한 나쁜 상황 때문에 미래를 계획하지 못하게 됩니다.

그래프에서 볼 수 있듯이 개인의 평균 급여 상승률은 인플레이션을 감안하면 그대로입니다. 사람들이 더 열심히 일했지만, 돈의 가치 하락 속도에 맞춰 임금 인상이 이루어지지 않고 있음을 의미합니다.

전 세계 사람들은 동일한 생활 수준을 유지하려고 더 많은 직업을 갖거나 더 오랜 시간 동안 일하게 됩니다. 마치 러닝머신 위에서 점점 더 빨리 달리지만, 앞으로 나아가지 못하는 것과 같습니다.

명목화폐 시스템은 사람들로 하여금 끊임없이 상승하는 물가와 경쟁하는 끝없는 경주에 갇혀 있는 듯한 기분이 들게 만듭니다.



제 5장

증가하는 비용 때문에 고군분투하는 많은 사람들은 신용에 의존하게 됩니다. 마치 큰 상처에 작은 반창고를 붙이는 것과 같습니다. 사람들은 생계를 유지하려고 대출을 받거나 갑작스런 결정을 내립니다. 사람들은 돈을 빨리 써야 하는 상황으로 몰리게 되어 내일을 계획하는 것보다 지금 당장 생존하는 것이 우선이 되는 악순환에 빠지게 됩니다.

명목화폐 시스템은 끊임없는 화폐 발행 때문에 사람 심리에 악 영향을 미칩니다. 짧은 기간 이익에 집중하고 오랜 기간의 계획을 희생하도록 강요합니다. 눈앞에 문제부터 해결하는 것처럼 명목화폐 세계 사람들은 눈앞의 이익을 우선시합니다. 이것은 인간의 생존 본능이라서 오랜 기간 이어질 수 있는 계획이 아니더라도 돈을 빨리 얻을 수 있다면 수단과 방법을 가리지 않게 되는 악순환이 반복됩니다.

결국 명목화폐 시스템 영향으로 전 세계의 사람들에게 벅찬 일을 해야 하는 현실을 만들어냅니다. 물가는 계속 오르고 소득은 정체되며, 살아남으려는 싸움은 날마다 이어집니다 일부 집단은 더 부유해지지만 사람들 대부분은 자신을 점점 더 가난하게 만드는 시스템에 의존하게 되는 상황에 놓이게 됩니다.

5.2.2 사회에 미치는 영향 – 증가하는 부의 불평등

건전화폐(sound money)에 기반한 사회에서 정부의 재정 결정은 국민의 승인이 있어야 가능합니다. 그러나 명목화폐 시스템에서는 정부가 국민들에게 부담을 주며 무제한으로 부채를 늘릴 수 있습니다.

정부가 원하는 대로 돈을 찍어낼 수 있는 권한은 정치 중앙집권화를 초래합니다. 명목화폐 시스템은 정부가 막대한 부채를 축적하고 자신들에게 유리한 결정을 내릴 수 있게 만듭니다. 때문에 미국과 같은 초강대국들은 경쟁에서 우위를 얻습니다. 이들은 끝없이 돈을 찍어서 전쟁과 자신들의 계획에 필요한 자금을 마련할 수 있으며, 강대국들로 하여금 지배력을 유지하고 영향을 미치며 지정학 갈등에 관여할 수 있도록 합니다. 초강대국들에게는 돈을 찍어낼 수 있으므로 전쟁과 타인을 통제하기 위한 것들이 가능하지만, 그렇지 못한 국가들은 결국 한계에 직면하게 됩니다.

명목화폐 시스템 하에서는 노력한만큼 부가 고르게 분배되지 않습니다. 대신 소수에게 집중되는 경향이 있습니다. 모노폴리 게임으로 비유하자면 한 플레이어가 모든 땅을 소유하고 다수는 살아남기 위해 계속 땅을 피하길 기도해야 하는 것과 같습니다.

돈을 찍어내는 행위는 정부와 중앙은행 간 긴밀한 협력을 통해 이루어지며, 새롭게 발행된 화폐의 수혜자는 부와 지위를 가진 강력한 기관과 개인들입니다. 이들은 새로 찍어낸 돈이 경제에 퍼져 경제 침체나 모두의 구매력 감소가 되기 전에 이미 모든 혜택을 누립니다.

문제를 어떻게 해결해야 하는가?

부가 평등하지 않은 것은 단순히 가진 자와 못 가진 자의 문제가 아닙니다.

결국 환경이 어려운 상태에 처한 사람들은 계층 사다리를 오르는 것이 점점 더 어려워지고 있으며, 무거운 배낭을 메고 경주를 시작하는 것과 같습니다. 부자와 가난한 사람들 간 격차가 커지면서 모든 사람들에게 문제를 초래하고, 정치인은 자신들에게 유리한 정책을 만들어냅니다. 결국 사람들에게 더 큰 부담을 주며, 사회 불안, 제도에 대한 불신, 그리고 카드로 쌓은 집처럼 공동체가 붕괴되는 결과를 낳습니다. 명목화폐 시스템 불안정성은 경제 불확실성, 정치 불안, 강대국이 경제 침체를 겪을 때 전세계로 퍼져 나타납니다.

이것은 선진국과 개발도상국을 막론하고 전 세계 사회에 영향을 미치는 글로벌 현상입니다.

때때로 부유한 개인과 집단은 이 기회를 이용해 글로벌 금융 시스템을 자신들에게 유리하게 활용하며, 이는 상류층과 하류층 간 격차를 더욱 벌어지게 합니다.

명목화폐 시스템 하에서는 빚을 지는 것이 세계 모든 사람에게 표준이 되었습니다. 정부, 기관, 기업, 개인 모두 막대한 빚에 빠져 있는 상황입니다.

빚을 용인하는 분위기는 명목화폐 시스템에 뿌리를 두고 있습니다. 지난 몇 십년 동안 많은 사람이 막대한 빚을 지는 것이 점점 쉬워졌으며 물가와 생활비가 올라서 모두에게 빚을 강요하게 되는 경우가 많습니다.

때문에 사람들이 필요한 것 이상을 소비하도록 유도하며 과소비와 낭비로 이어집니다. 끝나지 않는 쇼핑 축제처럼 보이지만 실제 지불해야 하는 비용은 숫자가 아니라, 사람들 심리와 건강에까지 영향을 미칩니다.

이로부터 알 수 있듯이, 명목화폐 시스템은 단순한 경제 메커니즘이 아니며 인간 사회 전체를 형성하는 시스템입니다. 권력의 집중에서 글로벌 역학, 재산 차이, 사회 규범에 이르기까지, 명목화폐 시스템은 국가 운영 방식과 사람들이 삶을 살아가는 방식에 직접 영향을 미칩니다.



체험 활동: 화폐 시스템의 결과

1. 명목화폐 시스템으로 인해 개인과 사회가 겪는 결과는 각각 무엇인가요?
2. 여러분들 국가에서 명목화폐 시스템의 결과는 무엇인가요? 과거에 어떤 일이 일어났으며, 그것이 사람들에게 어떤 영향을 미쳤나요?

제 5장

5.2.3 글로벌 부채 부담

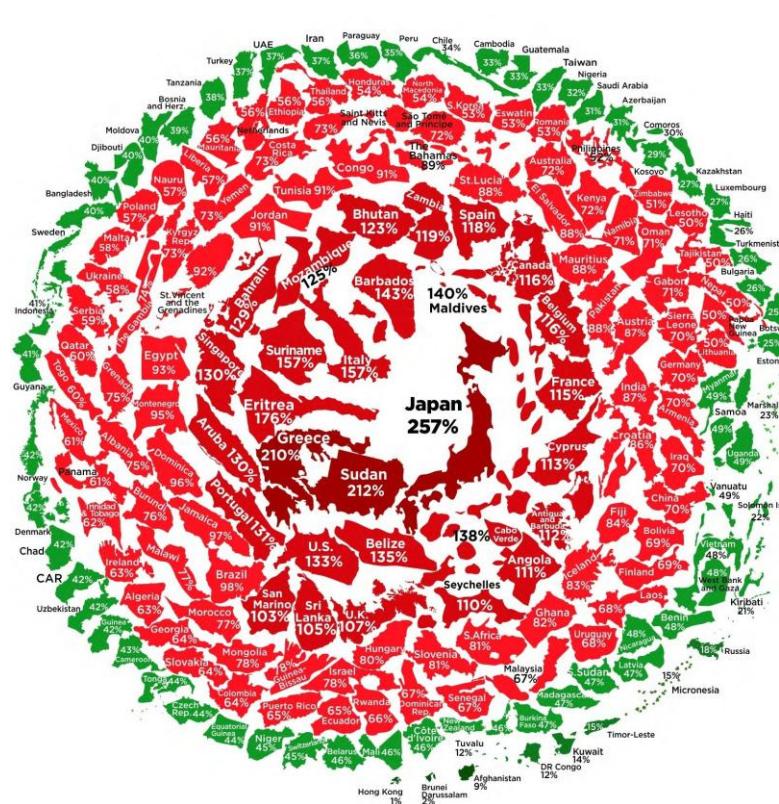
명목화폐 시스템 때문에 전 세계 정부들은 거대한 부채에 갇혀 있으며, 이것은 “글로벌 부채 소용돌이(Global Debt Spiral)”라 불립니다. 자신이 감당할 수 없는 돈을 계속해서 빌린다면 어떻게 될지 생각해보세요. 지금 전 세계에서 이런 일이 벌어지고 있습니다. 정부들은 막대한 부채에 빠져 있으며 절대 상환할 수 없는 수준의 빚을 계속해서 쌓아가고 있습니다. 이는 무분별한 지출과 대출, 미래를 위한 계획 부족이 만들어낸 결과이며, 현재 세계 각 국가를 파산 위기로 몰아넣고 있습니다.



미국 연방 정부는 2019년부터 현재까지 새로운 부채를 무려 1조 달러 이상 발행했습니다. 총 부채는 2019년 4분기 약 23조 달러였지만, 현재 34조 달러로 폭등했습니다.

전 세계 정부들이 새로운 부채를 쌓아내는 속도는 멈추지 않고 있으며 오히려 가속화되고 있습니다. 2023년은 2021년 코로나 팬데믹 시기 이후 가장 많은 부채가 추가된 해로 예상되었습니다.

세계 각국의 부채 현황



그렇다면 이미 명목화폐 시스템 결과를 감당해야 하는 개인과 사회에게 이것은 무엇을 의미할까요? 그들이 빠져 있는 부채 소용돌이는 마치 언덕 아래로 굴러가는 눈덩이와 같아서 점점 더 커지기만 하며, 멈춰야 할 방법을 모르는 상황입니다.

앞서 언급된 부의 불평등부터 사회 불안의 결과들은 사라지지 않을 것입니다. 오히려, 글로벌 부채 부담은 이제 돌아갈 수 없는 지점에 도달했으며, 상황이 더욱 악화될 것이 확실해 보입니다

2021년 부채 대비 GDP 비율 (%)



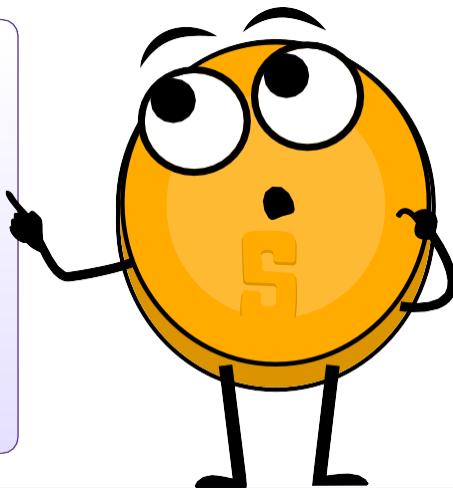
문제를 어떻게 해결해야 하는가?



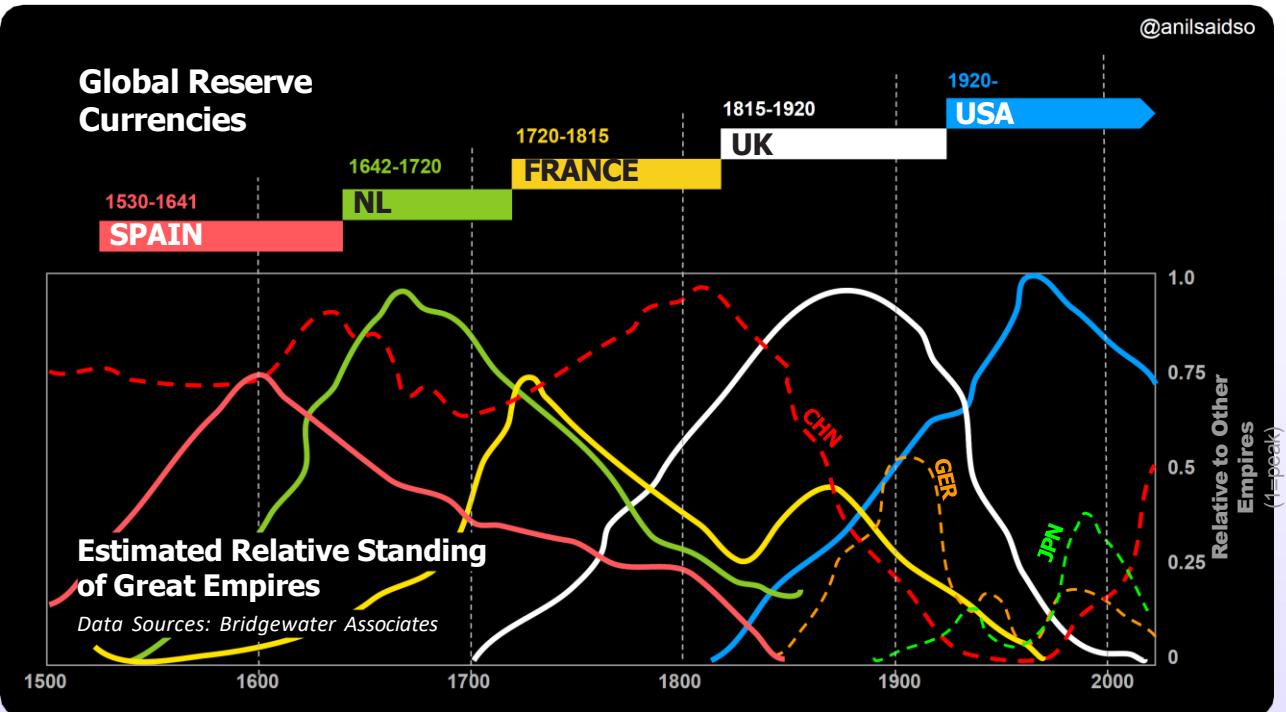
나는 정부의 손에서 화폐를 빼앗기 전까지는 좋은 화폐를 가지지 못할 것이라고 확신합니다. 우리가 할 수 있는 유일한 방법은 그들이 막을 수 없게 무언가를 우회하여 도입하는 것입니다.

프리드리히 하이에크

노벨 경제학 노벨상 수상자



Global Reserve Currencies



5.3 사이퍼펑크와 분산형 화폐가 걸어온 길

우리는 역사를 통해 은행과 정부에 의한 화폐 장악을 목격해 왔으며, 이것은 오늘날 우리가 알고 있는 명목화폐 시스템이며 사회에 미치는 악영향이 미치는 결과로 이어졌습니다. 그러나 암호화 기술과 인터넷과 같은 새로운 기술의 부상은 정부 개입에서 자유롭고, 모든 사람에게 열려 있으며 접근 가능한 디지털 화폐와 같은 새로운 아이디어가 등장할 수 있는 길을 열었습니다.

5.3.1 사이퍼펑크

“

컴퓨터는 사람들을 통제하는 것이 아니라, 해방시키고 보호하는 도구로 사용될 수 있습니다.

할 피니

”

20세기 후반에는 컴퓨터와 인터넷과 같은 여러 기술 혁신이 등장하며 새로운 디지털 시대의 길을 열었습니다.

이 그룹 사람들은 이러한 거대한 혁신이 사회가 작동하는 방식을 변화시킬 것임을 발견했습니다. 그들은 개인용 컴퓨터가 자유를 촉진하고 개인을 강화하는 도구가 될 잠재력 뿐 아니라, 완전한 통제와 감시의 도구가 될 위험성도 예견했습니다.

이들을 “사이퍼펑크(Cypherpunks)”라 불렸습니다. 사이퍼펑크는 활동가, 암호학자, 프로그래머, 프라이버시 활동가 그룹으로, 이들은 프라이버시, 보안, 그리고 분산화된 디지털 미래를 추구하는 공통된 비전을 공유했습니다.

“사이퍼펑크(Cypherpunk)”라는 용어는 암호를 뜻하는 “cypher”와 반문화의 반란 정신을 나타내는 “punk” 결합에서 유래했습니다.

사이퍼펑크들은 암호학이 개인의 자유를 보호할 수 있는 힘이 있다고 믿었습니다. 그들의 목표는 온라인 통신을 보호하고, 인터넷 활동을 익명화하며, 중앙집권 권력 통제를 벗어나 작동할 수 있는 디지털 화폐를 구축하는 것이었습니다.

사이퍼펑크들은 명목화폐 시스템 결과를 이해하고 “오웰리안(Orwellian) 미래” 위협을 보았습니다. 그들은 개인용 컴퓨터와 인터넷이 인류를 위한 선한 도구로 작용하도록 보장해야 하며, 국가가 국민을 통제하려는 도구로 전락하지 않도록 해야 한다고 믿었습니다.

오웰리안 미래의 정의:



오웰리안 미래는 조지 오웰(George Orwell) 작품에서 영감을 받은 디스토피아 비전을 가리킵니다. 정부 통제, 광범위한 감시, 정보 검열, 선전 선동, 조작 같은 전체주의 사회와 연관이 있습니다.

오웰리안(Orwellian)이라는 표현은 자유와 개인의 자율성이 심각하게 제한되고 모든 의견이 억압되며 강력하고 독재 정권 이익을 위한 왜곡된 시나리오를 묘사할 때 자주 사용됩니다.

이 개념은 조지 오웰 이름에서 따온 것으로, 그는 작품에서 고삐 풀린 정부 권력의 위험성과 천부 인권 침해의 잠재 위험에 대해 경고했습니다.

문제를 어떻게 해결해야 하는가?

사이퍼펑크 주요 인물로는 에릭 휴스(Eric Hughes), 티모시 C. 메이(Timothy C. May), 존 길모어(John Gilmore)와 같은 선구자들이 포함되었습니다. 1992년 에릭 휴스는 “사이퍼펑크 선언문(A Cypherpunk Manifesto)”을 작성하여 원칙을 명확히 했습니다. 이 선언문은 프라이버시, 암호화의 중요성, 그리고 개인이 디지털 정체성을 스스로 통제할 필요성을 강조했습니다.



“ ”

이 영상을 시청하고
사이퍼펑크들의
이야기를 들어보세요!

사이퍼펑크의 가장 주목할 만한 발명 중 하나는 암호화 도구 및 프로토콜 개발이었습니다. 1991년, 필 짐머만(Phil Zimmermann)은 이메일 암호화 소프트웨어인 PGP(Pretty Good Privacy)를 개발하였으며, 이는 사이퍼펑크를 나타내는 상징있는 프로젝트가 되었습니다. PGP를 통해 이메일 사용자는 오직 받는 사람만 해독할 수 있는 암호화된 메시지를 주고받을 수 있게 되었습니다. PGP가 개발되기 전에는 인터넷에서 전송된 모든 메시지가 정부를 포함한 제3자가 가로채고 읽을 수 있는 상태였기 때문에, PGP는 인터넷 보안의 빠른 발전을 이루어낸 기술이었습니다.

사이퍼펑크들은 암호화 기술, 인터넷, 그리고 컴퓨터 발전이 디지털 공간에서 분산형 네트워크를 구축하는 강력한 기반을 제공한다고 믿었습니다. 이를 통해 개인들은 중앙 기관의 개입 없이 인터넷에서 자유롭게 소통하고 거래할 수 있는 환경을 조성할 수 있었습니다.

사이퍼펑크들은 인류를 위해 더 밝은 미래를 만들어가는 올바른 방향으로 나아가고 있었습니다. 그들이 구축하려던 기술이 자유를 극대화하는 도구로 사용될 수 있도록 했고 통제 수단으로 변질되지 않도록 하는 것이 목표였습니다. 하지만 아직 분산형 네트워크와 디지털 화폐라는 두 가지 핵심 요소가 부족한 상태였습니다.

5.3.2 중앙화 시스템 vs. 분산형 시스템

중앙화 시스템: 하나의 권력, 많은 문제

중앙화된 시스템에서는 모든 것이 중앙 기관 중심으로 운영됩니다. 이러한 중앙 집중형 시스템 권위는 마치 도시 한가운데 솟아 있는 높은 빌딩과 같으며, 전체 시스템이 모든 것을 통제합니다.

2022년 캐나다에서 평화 시위가 벌어졌을 때 정부와 은행은 시위 참가자들의 계좌를 동결했습니다.

The image block contains two main parts. On the left, there is a photograph of several modern skyscrapers, likely the Shanghai World Financial Center and the Jin Mao Tower, symbolizing a centralized system where power is concentrated in a few large institutions. On the right, there is a 3D diagram of a network. It features a central blue cloud icon from which multiple lines of connection extend to six laptops arranged around it. This visualizes a decentralized network where individual devices (laptops) are connected to a shared central resource (the cloud), illustrating how data can be distributed rather than being controlled by a single central authority.



중앙화 시스템 문제점:

- ◆ 단일 실패점(Central point of failure): 만약 중앙 기관에 문제가 발생하면 전체 시스템이 붕괴할 수 있습니다.
- ◆ 통제(Control): 상층부 소수 집단이 모든 권력과 통제권으로 자신들에게 더 유리한 결정을 내립니다.
- ◆ 비효율성과 중개자(Inefficiency and intermediaries): 도시 교통 체증처럼, 중앙화된 시스템은 불필요한 중개자들 때문에 느려지고 비용이 증가할 수 있습니다.
- ◆ 자율성 부족(Lack of autonomy): 개인들은 금융 결정을 직접 내리지 못하며 모든 것이 상위 기관이 결정합니다.
- ◆ 검열과 제한(Censorship and restriction): 도시 일부 구역이 차단될 수 있는 것처럼, 중앙화 시스템은 특정 개인의 접근을 차단하거나 제한할 수 있습니다.
- ◆ 확장성 문제(Scaling challenges): 금융 서비스를 더 많이 필요로 할수록 중앙화 시스템이 감당하기 어렵습니다.
- ◆ 보안 위험(Security risks): 중앙 기관에 문제가 발생하면 전체 시스템이 사이버 공격 위험에 처할 수 있습니다.
- ◆ 투명성과 신뢰 부족(Lack of transparency and trust): 중앙화 시스템의 내부 작동 방식은 이해하기 어렵기 때문에, 사람들은 중앙화 시스템을 신뢰하기 어렵습니다.

분산형 시스템: 권력을 개인에게

이제 분산형 시스템을 거대한 숲과 비교해봅니다. 나무가 개별 부분을 나타내고 숲이 시스템을 구성합니다. 도심의 높은 빌딩처럼 중앙 기관이 있는 도시와는 달리 분산형 시스템은 마치 튼튼한 숲과 같아서 일부가 문제 생기더라도 전체 시스템은 계속 유지될 수 있습니다.

실제 사례:

Tor 네트워크와 브라우저는 사람들이 인터넷에서 익명을 유지할 수 있도록 만들어진 분산형 시스템입니다. 이 네트워크는 검열을 어렵게 만들며 사용자들이 자유롭게 인터넷을 사용할 수 있도록 합니다.



문제를 어떻게 해결해야 하는가?

분산화 시스템 장점:

- ◆ 강화된 복원력과 신뢰성(Enhanced resilience and reliability): 단일 실패점이 없기 때문에 일부에 문제가 발생하더라도 시스템이 강력하게 유지됩니다.
- ◆ 향상된 보안(Increased security): 적절한 암호화 및 보호 장치가 적용되면 단일 기관 권력의 통제와 검열에 저항하는 능력이 더욱 뛰어납니다.
- ◆ 더 많은 주권(Greater sovereignty): 개인이 돈, 데이터, 그리고 결정에 대해 더 많은 통제권을 가집니다.
- ◆ 개선된 투명성(Improved transparency): 모든 사람이 동일한 정보를 공유하기 때문에, 시스템 신뢰성이 높아집니다.
- ◆ 허가 없이 참여 가능하고 무한한 특성(Permissionless and limitless nature): 누구나 참여할 수 있고 모두에게 열려 있는 금융 시스템을 형성합니다.
- ◆ 동등한 기회(Equal opportunities): 모든 사람이 공정하게 기여할 수 있고 의견을 낼 수 있는 기회를 가집니다.
- ◆ 강화된 프라이버시(Enhanced privacy): 데이터가 여러 참가자들에게 분산되어 있고 대부분이 가명으로 처리되기 때문에, 분산형 시스템은 보다 높은 수준의 프라이버시를 제공합니다.

분산형 시스템은 많은 장점이 있지만, 모두 함께 결정을 내리는 과정은 다소 까다로울 수 있습니다. 이를 위해서 모든 참여자가 협력해야 합니다.

권력을 행사하는 방식 변화

중앙화된 시스템과 분산형 시스템이 공존하는 세계에서 가장 큰 차이는 권력이 누구에게 주어지는가에 있습니다. 중앙화 시스템은 소수 집단에게 권력을 집중시키지만 분산형 시스템은 권력을 분산시켜 모든 사람이 의견을 낼 수 있도록 합니다. 이러한 권력 이동은 더 공정한 미래를 의미하며, 많은 사람들이 자신의 삶에 영향을 미칠 수 있도록 합니다.

5.3.3 디지털 화폐의 간략한 역사

사이퍼펑크들이 논의한 가장 중요한 개념 중 하나는 “디지털 화폐(Digital Cash)”였습니다. 그들은 국가와 화폐를 분리하는 것이 미래 사회 공공 이익을 위해 필수라고 생각했습니다. 1980년대 데이비드 차움(David Chaum)은 안전하고 프라이버시가 보호되는 거래를 위한 암호화 프로토콜을 개발하며 혁신을 이루었습니다. 그러나 이 프로토콜은 중앙 기관이 모두 관리해야 한다는 단점이 있었으며, 단일 실패점(Single Point of Failure)과 검열(Censorship) 가능성이 제기되었습니다.

그 후 몇 년 동안 여러 사이퍼펑크들이 정부 통제를 받지 않는 디지털 화폐를 만들려고 서로의 아이디어를 발전시키며 해결책을 모색했습니다.

아래 표는 사이퍼펑크들이 디지털 화폐를 만들기 위해 개발한 주요 혁신들을 설명합니다.



제 5장

명칭, 날짜	설명	명칭, 날짜
E-Cash (1982)	데이비드 차움의 E-Cash는 초기 전자 화폐 개념으로, 암호화 기술을 통해 프라이버시에 중점을 둔 시스템입니다.	중앙 기관을 필요로 했으며, 단일 실패점과 검열 가능성 우려를 불러일으켰습니다.
DigiCash (1990)	데이비드 차움이 설립한 DigiCash는 프라이버시를 강조하는 디지털 화폐 형태를 만드는 것을 목표로 했습니다.	결국 중앙화된 모델이 1998년에 파산하게 되는 원인으로 작용했습니다.
B-money (1996)	웨이 다이(Wei Dai)가 제안한 익명 분산형 전자 화폐 시스템 이론이었습니다.	실제 구현이 부족했으며, 개념 아이디어만 남았습니다.
Hashcash (1998)	아담 백(Adam Back)이 개발한 작업 증명(proof-of-work) 시스템으로, 이메일 스팸과 서비스 거부 공격(DDoS)을 줄이기 위해 설계되었습니다.	디지털 화폐와 관련된 이중 지불(double-spending) 문제를 직접 해결하지 못했습니다.
Bit Gold (1998)	닉 재보(Nick Szabo)가 제안한 작업 증명 요소를 포함한 분산형 디지털 화폐 시스템을 묘사했습니다.	구현되지 않았으며, 이론으로만 남았습니다.
e-Gold (2004)	실제 금으로 뒷받침한 중앙화된 디지털 화폐로, 사용자가 e-Gold 단위를 사고, 전송할 수 있도록 했습니다.	법적 문제로 인해 2009년에 폐쇄되었으며, 디지털 화폐는 중앙화되면 안된다는 교훈을 남겼습니다.

사이퍼펑크들이 수십 년 동안 특정 그룹이나 정부 통제를 받지 않는 디지털 화폐를 만들려고 수많은 시도를 했지만, 결국 한계에 부딪혔고 현실 세계에서 완전히 구현되지 못했습니다. 사이퍼펑크들은 안전하고, 확장 가능하며, 널리 채택될 가능성이 있는 디지털 화폐를 구축하는 것이 쉽지 않다는 결론에 도달했습니다.

그러나 이름 모르는 어떤 누군가가 사이퍼펑크들의 교훈을 배우고 분산형 디지털 화폐 개념을 새로운 차원으로 발전시켰습니다. 다음 장에서는 40년에 걸친 선행 연구를 기반으로 새로운 금융 시스템을 창조하는 데 성공한 역사를 살펴보겠습니다.

제 6장

비트코인 소개

6.0 사토시 나카모토의 비트코인 창조

6.1 비트코인은 작동 원리는 무엇인가?

6.1.1 나카모토 합의 알고리즘

6.1.2 게임의 참여자들

체험 활동: 개인 대 개인 네트워크에서 합의 형성

6.2 디지털 건전화폐인 비트코인

6.2.1 서론

6.2.2 비트코인의 특징

체험 활동: 수업 토론 - 비트코인은 건전화폐인가?

6.2.3 책임과 권한을 이해하기

학습 워크북

한국어 버전 | 2025

비트코인 소개

6.0 사토시 나카모토의 비트코인 창조

“

1990년대 이후 모든 기업들이 실패한 모습을 보고 전자화폐가 필요 없다고 합니다.

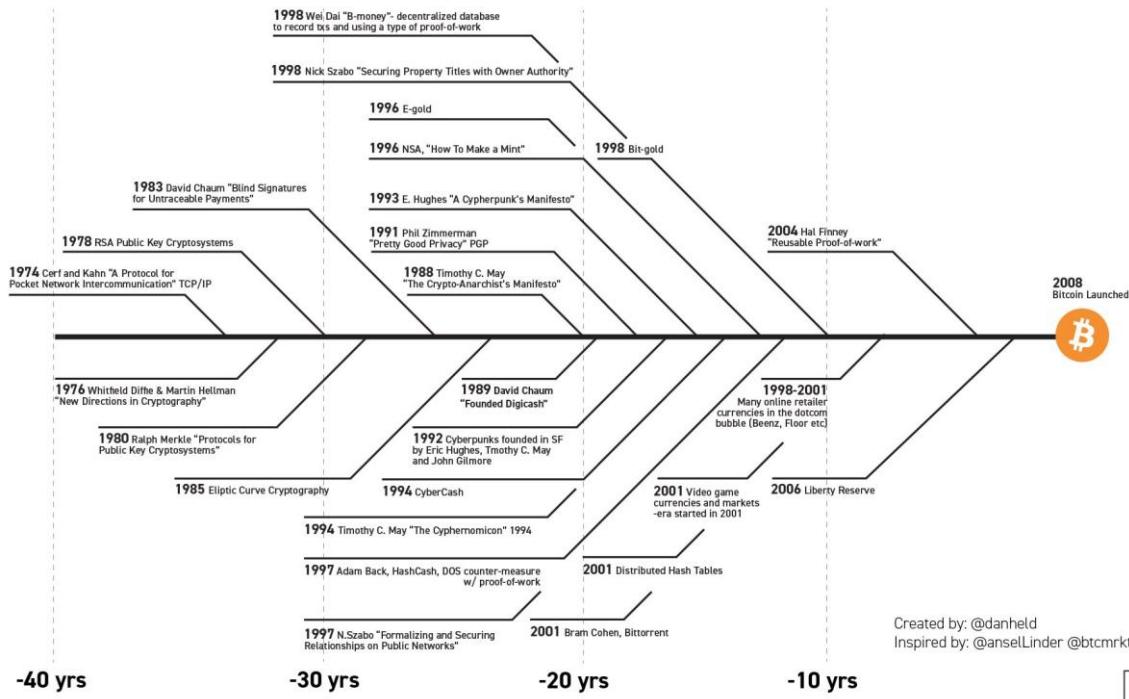
하지만 그것들은 중앙 통제되는 특성 때문에 망한 것 입니다.

저는 비트코인이 분산화되고 비신뢰 기반 시스템을 시도하는 첫 번째 사례라고 생각합니다.

사토시 나카모토

”

Bitcoin prehistory - It's the result of 40 years of research, development and demand



여러 사이퍼펑크들은 대안 화폐 시스템을 만들려고 노력했습니다. 이번 장에서는 그들 중 한 명, “사토시 나카모토(Satoshi Nakamoto)”라는 시대를 앞서 나가는 주인공 이야기를 이어갑니다.

이 익명의 인물(남성, 여성, 혹은 그룹)은 비트코인이 등장하기 훨씬 이전부터 컴퓨터 과학자와 해커들과 같은 암호학 매니아들 사이에서 명목화폐 시스템을 대체할 실제 해결책을 찾기 위한 논의에 참여했던 사람 중 하나였습니다.

Page: [1] Author Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 25115 times)
Added some DoS limits, removed safe mode (0.3.19)
December 12, 2010, 06:22:39 PM
Merit by: EFS (20), jingqiu (15), Optibay (50), bankcoin (450), doverone (55), reggaemanhattan (65), sammamish (15), shahid (227), netrek (25), Welsh (20), midnurst (20), AlCrib (11), dragonvirus (11), legenddr (10), harymann (10), artilz (7), Betwong (5), Meepurinis (5), Laudo (5), Morobay (5), TMAN (5), Stetey (5), minorman (5), TrueGreeds (4), Danilip (3), finski (3), Ryu_Ari (3), Youffree (2), Btha (2), iDiva (2), Dzheron (2), Saito (2), Kite (2), kyle (2), jay (2), hapehe99 (1), Sealing (1), bitcoinhyde (1), DmtrRus (1), d1gital (1), goldingerone (1), jamaicamuerto (1), crypt_trader#43xExP (1), billgates (1), derzikim (1), DaCryptoAccoun (1), uogli (1), eXtreme (1), iefom (1), ryap12 (1), CoolWave (1), mx12_levin (1), gieran (1), nikolospolo (1), lchz (1), TheArchaeologist (1), rhoncience (1), murayabead (1), akopjorge (1), sign44 (1), OWZ2337 (1), llecon (1), zanteus (1), Tech3k (1), EKAloji (1)

There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19.

- Added some DoS control
As Gavin and I have said clearly before, the software is not at all resistant to DoS attack. This is one improvement, but there are still more ways to attack than I can count.

I'm leaving the -limittfreetrelay part as a switch for now and it's there if you need it.

- Removed "safe mode" alerts
"safe mode" alerts was a temporary measure after the 0.3.9 overflow bug. We can say all we want that users can just run with "-disablesafemode", but it's better just not to have it for the sake of appearances. It was never intended as a long term feature. Safe mode can still be triggered by seeing a longer (greater total PoW) invalid block chain.

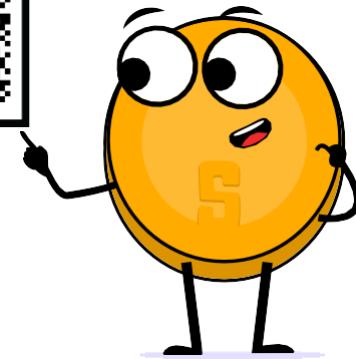
Builds:
<http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/>

제 6장



2008년 10월, 사토시 나카모토는 “비트코인: 개인 대 개인 전자 화폐 시스템(Bitcoin: A Peer-to-Peer Electronic Cash System)”이라는 백서를 암호학 메일링 리스트에 공개했습니다. 이 문서는 중개자 없이 안전한 온라인 거래를 가능하게 하는 분산형 P2P 프로토콜 기초를 마련했습니다.

그의 비전은 명확했습니다. 강력한 정부와 금융 기관 통제로부터 자유로운, 순수한 P2P 방식의 전자 화폐를 만드는 것이었습니다.



2009년 1월 3일 사토시 나카모토는 “제네시스 블록(genesis block)”으로 알려진 첫 번째 비트코인 블록을 채굴했습니다. 이는 분산형 원장을 통해 신뢰와 보안을 기반으로 구축된 새로운 화폐 시스템인 비트코인 네트워크의 공식 출범을 의미했습니다.

그 후 점점 더 많은 열정있는 사람들이 이 아이디어에 동참하고 기여하기 시작했습니다.

비트코인 제네시스 블록

16진수 버전

00000000	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00;Eifz({^zC,>
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	gv.a.B.^SQ2;V,a
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	K.^J)=_Iyy.+
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C
00000050	01 01 00 00 01 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1DyyyyM.yy..
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..The Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 68 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6B 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksyyyy..o.
000000D0	2A 01 00 00 04 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gS^pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0..\\ð'^(à9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EP 38 C4	ybaé.ab^ið?Lí8A
00000100	F3 55 04 E5 1B C1 12 DE	5C 38 4D F7 BA 0B BD 57	óU.å.þ\SM+9..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._-....

사토시 나카모토는 2011년 비트코인 네트워크가 창시자 영향 없이도 실패 없이 운영될 수 있음을 입증한 후, 한 비트코인 개발자에게 이메일을 보내 비트코인에서 손을 떼고 그 미래를 자신과 비전을 공유하는 “믿을 만한 손”에 맡기겠다고 발표했습니다.

사토시 나카모토 정체는 오늘날까지도 미스터리로 남아 있지만 비트코인을 만든 목적만큼은 결코 미스터리가 아니었습니다. 소수에게 집중된 권력을 분산화된 오픈소스의 투명한 화폐 시스템으로 대체하여 다수에게 되돌려주려고 비트코인을 만들었습니다. 즉 화폐를 국가에서 분리하기 위한 대안을 제시한 것입니다. 그는 2008년 금융위기 해답으로 비트코인을 만들었습니다. 이 위기는 전 세계 모든 사람들에게 큰 고통을 주는 동시에 또다시 엘리트 계층을 부유하게 만들었습니다. 비트코인은 사토시 나카모토가 화폐 시스템 부패와 취약성에 답한 것이었습니다. 그렇게 새로운 혁명의 토대를 세웠지만, 그 공로를 주장하지 않고 조용히 물러났습니다.

비트코인 소개

이후 몇 년 동안 비트코인은 빠르게 성장하며 화폐 시스템에 도전하며 안전하고 검열에 저항할 수 있는 금융 거래 수단을 제공했으며, 희망과 회복력의 상징으로 자리 잡았습니다. 비트코인은 오픈소스 프로토콜로 그 누구도 소유하거나 통제할 수 없습니다. 비트코인 설계는 모두 공개되어 있으며 누구나 참여할 수 있습니다.

오늘날 비트코인 덕분에 국경 없이 투명하고 안전한 금융 시스템의 꿈은 여전히 살아 숨 쉬며, 우리가 목격하고 있는 글로벌 자유 혁명에 힘을 실어주고 있습니다. 매일 평범한 사람들은 명목화폐 시스템에서 벗어나 비트코인 세계로 이동하고 있습니다. 전 세계 곳곳에서 자유를 열망하는 사람들이 비트코인으로 지속 가능 경제를 만들고 있습니다. 심지어 엘살바도르와 같이 대안을 찾고자 하는 국가들도 각자의 방식으로 비트코인을 채택하기 시작했습니다.

6.1 비트코인은 어떻게 작동할까요?

6.1.1 나카모토 합의 알고리즘

그렇다면 비트코인이 작동하는 원리는 무엇일까요? 비트코인은 다양한 기능이 있으며 구조는 매우 깊고 복잡합니다. 그럼에도 처음 비트코인 세계에 들어선 사람들에게 비트코인 기술을 이해하지 못하더라도 문제없이 사용할 수 있습니다.

마치 인터넷을 사용하는 것과 비슷합니다. 대부분의 사람들은 TCP/IP 프로토콜이 작동하는 기술은 모르지만, 매일 이메일을 보내고 메시지를 주고받으며 소셜 미디어에 게시물을 올립니다. 자동차를 운전하는 것도 마찬가지입니다. 대부분 사람들은 자동차가 작동하는 원리를 자세히 모르지만, 운전하는 방법은 알고 있습니다.



그러나 비트코인은 아직은 널리 채택되지 않았습니다. 1990년대 인터넷처럼 새로운 기술이기 때문입니다. 따라서 비트코인 기본 개념을 기술기반이 아닌, 좀 더 쉬운 방식으로 이해하는 것이 도움이 될 수 있습니다.

제 6장

비트코인이 작동하는 핵심 개념을 한 문장으로 요약하면 다음과 같습니다. 비트코인은 온라인에서 사람들이 맺는 합의(agreement)입니다. 비트코인을 친구들과 함께 하는 보드게임(모노폴리)에 비유해 보겠습니다. 플레이어들은 미리 정한 게임 규칙에 동의해야 합니다. 모노폴리 규칙 중 하나는 “모노폴리 지폐”만 유효한 화폐로 인정된다는 것입니다. 만약 플레이어 중 한 명이 규칙을 어기고, 모노폴리 지폐 대신 화장지를 사용해 집을 사려고 한다면 다른 플레이어들은 아무도 그와 함께 게임을 하지 않을 것입니다. 즉, 게임을 하려면 모든 플레이어들이 동일한 규칙에 합의해야 하며, 그 규칙에서 벗어나는 사람은 받아들여지지 않는 것입니다.

이것이 비트코인이 작동하는 방식과 실제로 같습니다. 비트코인은 동일한 규칙을 따르는 사람들로 구성된 네트워크입니다. 이 규칙들은 수학으로 정의되어 있으며, 컴퓨터 코드로 작성되어 있고 비트코인 소프트웨어를 실행하는 모든 사람들이 수용합니다. 비트코인 규칙은 모든 참가자에게 동일하게 적용되므로, 누구나 이 규칙을 따르지 않으면 네트워크에서 거부당해 참여할 수 없습니다.

예를 들어 비트코인 규칙 중 하나는 비트코인 총량은 절대 2,100만 개를 초과할 수 없다는 것입니다. 만약 누군가 100만 개의 비트코인을 추가로 생성하려고 한다해도 그 시도는 아무런 의미가 없습니다. 비트코인 네트워크 모든 참여자들이 즉시 그를 식별하고 거부하기 때문입니다. 이러한 원칙이 비트코인을 강력하고 신뢰할 수 있는 시스템으로 만드는 요소입니다.

여러분이 누구인지, 어디에서 왔는지는 중요하지 않습니다. 비트코인 세계에 들어오려면 모든 사람들과 동일한 규칙을 따라야 합니다.

이 원칙은 명목화폐 세계에서 막대한 권력과 영향력을 가진 사람들과 기관들에게도 동일하게 적용됩니다. 비트코인 세계에서는 속임수나 방해 행위가 용납되지 않습니다. 모든 사람은 동등하게 대우받으며, 그 누구도 바꿀 수 없습니다.

알고 계셨나요?

2009년 이후로 비트코인은 수만 건에 달하는 해킹, 조작, 변경 시도를 견뎌냈습니다. 비트코인은 그 누구도 이를 멈추거나, 통제하거나, 조작할 수 없다는 것을 증명해냈습니다.



비트코인 소개

6.1.2 게임의 참여자들

비트코인 분산화(decentralization)를 더 잘 이해하기 위해서는 네트워크 내에서 각기 다른 역할을 수행하는 참여자들을 깊이 있게 살펴볼 필요가 있습니다. 비트코인 세계에서는 다양한 참가자들이 서로 다른 역할을 맡으면서도 조화롭게 협력하며, 네트워크가 원활하게 작동할 수 있도록 기여합니다.

1. 채굴자(Miners): 보안의 설계자

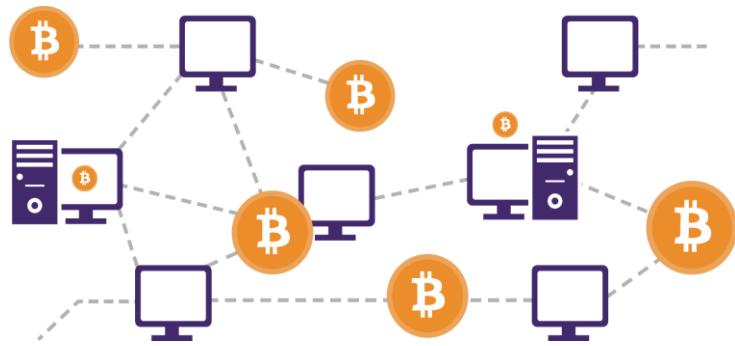
채굴자는 비트코인 핵심(backbone)을 담당하는 존재입니다. 이들은 작업 증명(Proof-of-Work, PoW)이라는 메커니즘을 통해 비트코인 네트워크를 유지하고 보호하는 보이지 않는 곳에서 활동하는 사람들 또는 그룹입니다. 채굴자들은 강력한 연산 능력을 가진 특수 컴퓨터를 사용하여, 하드웨어를 비트코인 네트워크에 연결합니다. 이들은 전 세계 사람들과 경쟁을 펼치며, 비트코인 분산 원장(타임체인)에 새로운 거래 블록을 추가하려고 경쟁하는 복권과 같은 시스템에 참여합니다. 이들의 헌신이 있는 노력 덕분에 비트코인 원장 불변성(immutability)이 유지되며, 의도를 가진 공격에도 네트워크가 안전하게 보호됩니다.



비트코인 채굴의 분산된 특성 덕분에, 충분한 연산 자원을 가진 사람이라면 누구나 채굴에 참여할 수 있습니다. 채굴자들은 복잡한 연산 문제를 가장 빠르게 해결한 대가로 비트코인을 보상 받습니다. 비트코인 채굴자는 전 세계에 분포되어 있어, 네트워크가 중앙화되는 것을 방지하고 비트코인 보안이 강력하고 분산된 상태로 유지되도록 보호하는 역할을 합니다.

2. 노드(Nodes): 검증의 수문장

비트코인 노드는 전 세계에 흩어져 있는 평범한 사람들입니다. 이들은 비트코인 네트워크 수문장(gatekeepers) 역할을 하며, 비트코인 소프트웨어를 실행하는 작은 컴퓨터에서 전체 원장(ledger) 사본을 유지합니다. 노드는 거래를 검증하며, 모든 참가자들이 합의된 규칙(consensus rules)을 준수하는지 확인합니다. 노드 네트워크에 검증 책임을 분산시킴으로써, 비트코인은 공격 저항력을 유지하고, 신뢰가 필요 없는(trustless) 시스템으로 작동할 수 있습니다. 노드는 비트코인 원장 무결성(integrity)을 유지하는 중요한 역할을 하며, 비트코인의 분산화 정신을 지키는 데 기여합니다.



제 6장



3. 사용자(Users): 권한을 가진 참여자

사용자는 비트코인 네트워크 핵심이며, 비트코인을 사용하는 개인들입니다. 사용자는 평범한 삶을 살아가면서도, 비트코인을 활용함으로써 스스로에게 더 많은 권한을 부여한 사람들입니다. 예를 들어 어떤 사용자들은 비트코인을 저축 수단으로 사용하고, 엘살바도르 시민들과 같은 일부 사용자들은 비트코인을 이용해 식료품을 구매하고 급여를 지급받습니다.

비트코인은 은행과 정부 같은 중개자 필요성을 없애고, 개인 대 개인 거래를 직접 가능하게 함으로써 사용자들에게 더 큰 자유를 제공합니다. 이는 사용자가 돈과 거래를 완전히 통제할 수 있음을 의미합니다.

4. 개발자와 프로젝트(Developers and Projects): 혁신의 설계자

미래 화폐 시스템은 스스로 만들어지지도 않으며, 올바르게 전 세계에서 채택되기 위해서는 끊임없는 노력이 필요합니다. 바로 여기에서 비트코인 개발자와 프로젝트가 중요한 역할을 합니다.

개발자들은 기술 전문성을 활용하여 비트코인 프로토콜을 개선하고 혁신합니다. 이들은 코드를 기여하고, 개선을 제안하며, 보안 취약점을 해결함으로써 비트코인 네트워크가 다양한 도전에 대응할 수 있도록 계속 발전하도록 만듭니다. 비트코인 오픈소스(Open-source) 특성은 전 세계 개발자들이 협력하여 성장할 수 있도록 합니다.

이러한 분산된 개발 구조는 단일 주체가 프로토콜을 통제하는 것을 방지하며, 합의(consensus)기반 과정을 통해 변경됩니다. 개발자들은 아이디어와 개선안을 제안하며, 최고 아이디어만이 비트코인 커뮤니티의 지지를 얻어 반영됩니다. 이를 통해 비트코인은 80억 인구를 위한 투명하고 모두를 위한 화폐로 발전해 나갑니다.

비트코인 프로젝트에는 비트코인 비전을 공유하는 다양한 그룹들이 참여합니다. 이들은 비트코인 도입을 촉진하고, 자유를 지향하는 글로벌 목표를 향해 함께 나아갑니다.

비트코인의 오케스트라: 조화로운 협력

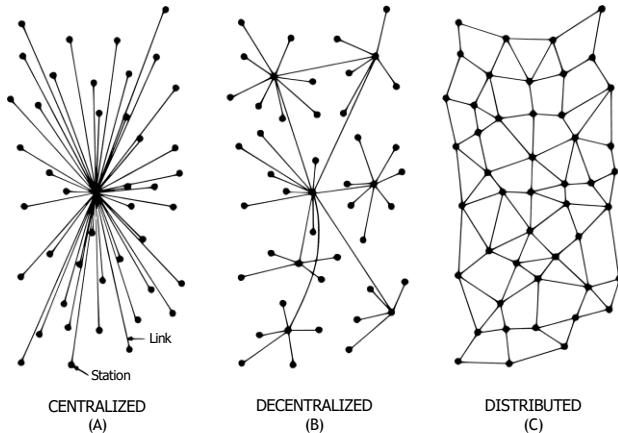
비트코인 분산화는 마치 하나의 조화로운 오케스트라와 같습니다. 각기 다른 연주자들이 협력하여 아름다운 음악을 만들어내는 것과 같은 원리입니다. 비트코인 네트워크에는 최고 권위자가 존재하지 않으며 채굴자, 노드, 사용자, 개발자, 프로젝트가 각자의 역할을 자유롭게 수행하면서도 협력하여 작동합니다.

노드가 유지하는 분산 원장은 투명성을 보장하며, 작업 증명(Proof-of-Work) 메커니즘은 보안을 제공하고 채굴 중앙화를 방지합니다. 사용자는 화폐 시스템 통제에서 벗어나 금융 주권과 자유를 경험합니다. 개발자들은 합의를 기반으로 프로토콜을 개선하며, 변화하는 시스템을 충족시키기 위한 네트워크가 적응할 수 있도록 보장합니다. 비트코인 프로젝트는 고유한 방식으로 모두의 자유를 위한 더 큰 목표에 기여하고 있습니다.

비트코인 소개

모든 참가자들은 비트코인 도입을 추진하고 인류에게 권한을 부여하는 데 중요한 역할을 합니다. 분산된 오케스트라의 각 참가자는 비트코인 복원력과 지속 가능성에 기여하며, 신뢰가 필요 없고 국경을 초월한 권한을 부여하는 생태계를 만들어갑니다.

따라서 비트코인의 분산화된 오케스트라 교향곡은 사토시 나카모토의 비전과 자유와 권한을 추구하는 글로벌 커뮤니티의 뜨거운 열정을 보여주는 증거이며 울려 퍼지고 있습니다.



체험 활동: 개인 대 개인 네트워크에서 합의 형성

목표



그룹 내에서 합의(consensus)가 이루어지는 원리를 이해하고, 암호화(cryptography)와 비트코인 합의 계층(consensus layer)에 대해 학습합니다.

자료



암호화(encrypted) 및 암호화되지 않은(unencrypted) 행동 지침이 포함된 메시지 (예: “공격” 또는 “공격하지 않는다”).

활동 준비



선생님은 다음 활동에서 나쁜 의도를 가진 노드(malicious nodes)가 될 학생 3~4명을 수업 전에 선정합니다. 그리고 이 나쁜 의도를 가진 노드들에게 암호화 숫자를 미리 알려줍니다.



제 6장

체험 활동: 개인 대 개인 네트워크에서의 합의 형성

1

교사는 그룹에서 한 명을 발신자(originator)로 선정하여, “공격”이라고 적힌 종이들과 나쁜 의도를 가진 노드가 미리 알고 있는 암호화된 “4-16-14-21-1-21-21-1-3-11” 숫자가 적힌 종이들을 줍니다.
(암호화된 숫자는 공격금지를 뜻합니다)

2

학생들은 지정된 공간에서 원 모양으로 앉으며, 나쁜 의도를 가진 노드 역할을 맡은 학생들이 중간에 섞이도록 배치합니다.

나쁜 의도를 가진 노드

나쁜 의도를 가진 노드



3

발신자는 쪽지를 원 오른쪽에 있는 사람에게 전달하며, 받은 사람은 다시 오른쪽에 있는 사람에게 전달합니다.

4

모든 사람이 메시지를 읽은 후에 발신자는 “지금”이라고 말하며 그룹에 신호를 보냅니다. 그룹은 이 메시지에 따라 동시에 움직입니다. 메시지가 “공격”이라고 적혀 있다면, 모든 참가자는 한 걸음 앞으로 나아갑니다.

5

암호화된 메시지를 알고 있는 나쁜 의도를 가진 노드는 가만히 있는 반면, 나머지 학생들은 암호화된 메시지를 모르므로 되어 합의(consensus) 부재를 드러냅니다.

비트코인 네트워크와의 연관성:

이 체험 활동을 통해 비트코인 네트워크에서 노드 간 합의(consensus)가 깨지면 발생할 수 있는 문제를 이해할 수 있습니다. 나쁜 의도를 가진 노드 때문에 합의가 이루어지지 않으면, 시스템이 제대로 작동하지 않는 것을 확인합니다.

비트코인 소개

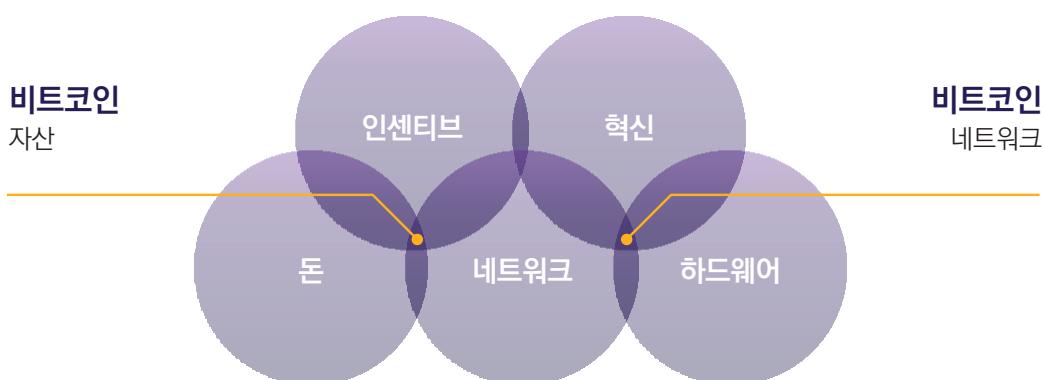
6.2 디지털 건전화폐인 비트코인

6.2.1. 서론



비트코인은 화폐입니다. 비트코인은 투자 수단이 아니라, 여러분이 열심히 벌어들인 돈을 안전하고 자유롭게 저축할 수 있는 방법입니다.

비트코인을 소유한다고 해서 부자가 되는 것은 아닙니다. 비트코인이 주는 가치보다 더 많이 주지 않기 때문입니다. 비트코인 가치는 명목화폐에 대비해 상승할 수 있지만, 단지 비트코인의 채택이 증가하고 명목화폐 가치가 하락하기 때문입니다.



비트코인은 새로운 형태 화폐로, 인터넷의 돈(The Internet of Money)이라 불립니다. 누구나 참여할 수 있으며, 다른 사용자들과 가치를 교환할 수 있는 열린 시스템을 의미합니다. 세상에서 가장 고립되고 가난한 사람도 금융 시스템에 접근할 수 있게 되었습니다. 마치 인터넷과 휴대전화만 있다면 누구나 검색 엔진을 사용할 수 있듯이, 비트코인은 휴대전화와 인터넷 연결만으로 새로운 글로벌 금융 시스템에 접근할 수 있는 가능성을 제공합니다.



빠르고
저렴한
지불수단

매우 낮은 수수료로 돈을 몇 분 안에 전세계로 송금합니다.



금융
포용

은행 계좌가 없는 25억 명의 사람들이 스마트폰이나 컴퓨터를 통해 금융 서비스를 이용할 수 있습니다.



향상된
프라이버시

비트코인 거래는 공개되지만,
신원은 공개되지 않습니다.

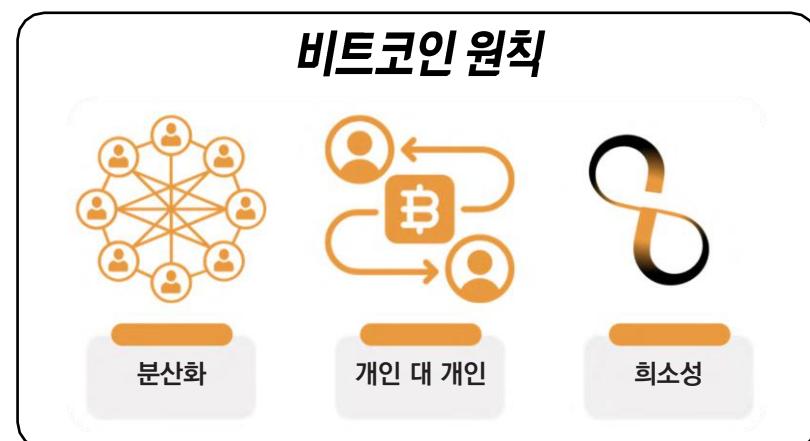


제 6장

비트코인은 완전히 디지털화 되어 있고 국경이 없습니다. 어디에 있든 전 세계의 컴퓨터와 스마트폰 위에서 작동합니다. 전 세계 많은 사용자들이 비트코인 소프트웨어와 원장의 사본을 실행하며 보유하고 있습니다.

소프트웨어와 모든 거래 기록은 수많은 사본이 존재하기 때문에 사라질 가능성이 거의 없습니다. 비트코인을 완전히 소멸시키려면 인터넷 전체를 영원히 차단해야 하는데, 이것은 일어날 가능성이 거의 없기 때문입니다.

비트코인은 희소성이 있습니다. 존재할 수 있는 비트코인 개수가 완벽하게 제한되어 있다는 뜻입니다. 가장 강력한 정부나 금융 기관조차도 비트코인을 위조할 수 없습니다.



6.2.2 비트코인의 특징

건전화폐의 진화

2장에서 배운 것처럼, 건전화폐 수명 주기는 사회에서 수용되기까지 세 가지 단계를 거칩니다. 가치 저장 수단(Store of Value)에서 시작해 교환 수단(Medium of Exchange)으로 전환되며 마지막으로 회계 단위(Unit of Account)가 됩니다.

화폐의 첫 번째 단계인 가치 저장 수단은 통화가 시간이 지나면서 안정적인(또는 가치가 상승하는) 자산으로 신뢰를 얻기 시작하는 단계입니다. 일찍 알아차린 사람들은 지정학, 경제의 불확실성이 있는 시기에 부를 보호하려고 이러한 화폐에 저장합니다.

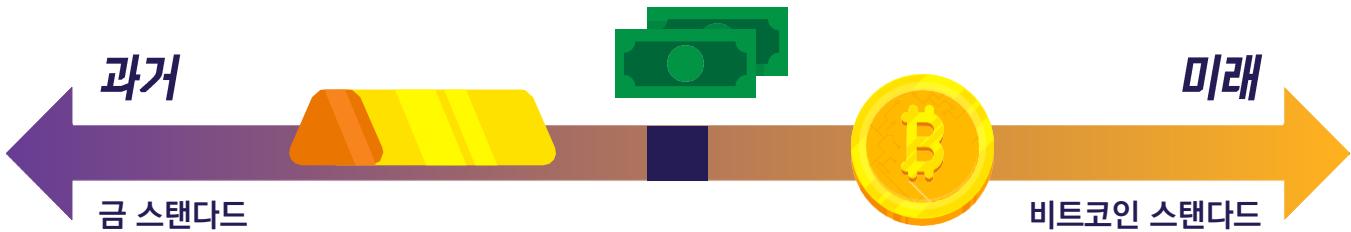
미디어 매체들은 비트코인을 디지털 금이라고 부릅니다. 지난 10년 동안 비트코인이 가치 저장 수단으로서 확고히 자리 잡았습니다. 매일 점점 더 많은 사람들이 비트코인을 금이 그랬던 것처럼 인플레이션의 해지 수단으로 보고 있습니다.

다음 단계는 화폐 안정성의 신뢰가 확고히 다져지는 시점입니다. 이때부터는 교환 수단으로 전환되며, 일상생활에서 거래를 용이하게 만듭니다. 이 단계에서 화폐는 재화와 서비스의 교환에 널리 수용되기 시작합니다.

비트코인은 점차 교환 수단이 되어가고 있습니다. 상인들이 비트코인을 받기 시작하고, 프로토콜이 발전함에 따라 비트코인 거래는 일상 활동에서 점점 더 편하고 흔한 일이 되고 있습니다.

엘살바도르는 그중 한 가지 예로, 비트코인을 법정 통화로 공식 인정한 국가입니다. 매일 더 많은 평범한 시민들과 기업들이 비트코인을 교환 수단으로 사용하고 있습니다.

비트코인 소개



마지막 단계에서 화폐는 회계 단위(Unit of Account)로서의 지위를 얻게 되며, 재화와 서비스 가격을 책정하는 척도로 사용되는 것을 의미합니다. 이 단계에서는 모든 상품들이 회계 기준으로 측정되는 표준 단위가 됩니다.

회계 단위로 자리 잡는 과정은 굉장히 오래 걸리는 여정입니다. 현재는 재화와 서비스를 오직 명목화폐로만 측정하고 있기 때문에, 비트코인은 더 넓은 채택과 다양한 금융 시스템과 통합이 필요합니다.

그러나 개인과 기업들이 점점 비트코인을 가치 기준으로 생각하고, 가격을 표시하기 시작하면서 기반이 다져지고 있습니다.



비트코인은 건전화폐의 진화 과정에 있습니다. 비트코인이 글로벌 금융 시스템에 완전히 통합되면 표준 회계 단위가 되어 전 세계 화폐 시스템을 재편할 가능성이 있습니다.



제 6장

화폐의 속성

2장에서 배운 것처럼 인류는 시간이 지남에 따라 진정한 건전화폐가 되기 위해 갖추어야 할 몇 가지 속성을 알아냈습니다. 이 속성들은 내구성(durability), 분할 가능성(divisibility), 휴대성(portability), 수용성(acceptability), 희소성(scarcity), 그리고 대체 가능성(fungibility)입니다. 이제 비트코인이 이 조건을 충족하는지 확인해봅시다.

내구성: 비트코인은 디지털 형태이기 때문에 완벽한 내구성을 갖추고 있습니다.

분할 가능성: 미국 달러(USD)는 센트(0.01) 단위로 나눌 수 있습니다. 비트코인은 사토시(Sat)로 알려진 단위로 나눌 수 있으며, 이것은 0.00000001 BTC를 의미합니다. 또한 비트코인은 디지털로 존재하기 때문에, 필요하다면 미래에는 더 세분화될 수도 있습니다. 현재 비트코인은 세계에서 최고로 분할 가능한 화폐 자산입니다.

휴대성: 2020년 4월 11억 달러(\$1.1 billion)가 단 몇 분 만에 전송되었으며, 수수료는 단 68센트였습니다. 이처럼 큰 금액을 매우 낮은 비용으로 신속하게 이동할 수 있는 다른 방법은 없습니다. 그리고 이 모든 과정이 중개자 없이 이루어졌습니다. 이것이 비트코인이 세계에서 가장 쉽게 이동할 수 있는 화폐인 이유입니다.

수용성: 비트코인은 아직 교환 수단(Medium of Exchange)으로 자리 잡는 초기 단계에 있으며, 명목화폐와 비교했을 때에는 아직 낮은 편입니다.

희소성: 비트코인은 최대 2,100만 개만 존재하도록 설계되었습니다. 최대 발행량을 코드로 제한하고 있으므로, 비트코인은 단순히 희소한 것이 아니라 세계에서 가장 희소한 화폐 자산입니다.

대체 가능성: 비트코인 최소 단위는 모든 비트코인의 최소 단위와 동일하며, 비트코인 프로토콜을 통해 동일한 가치로 교환 및 거래될 수 있습니다. 이러한 특성 덕분에 비트코인은 대체 가능한 화폐가 됩니다.

비트코인 소개

비트코인 vs 금 vs 달러

돈의 속성	금	명목화폐	비트코인
내구성	높음	중간	높음
휴대성	중간	높음	높음
분할성	중간	중간	높음
대체 가능성	높음	높음	높음
희소성	중간	낮음	높음
검증성	중간	중간	높음
역사성	높음	중간	낮음
검열 저항성	중간	중간	높음
프로그래밍 가능성	낮음	중간	높음

비트코인 vs 금 vs 미국 달러, 출처: Bitcoin Magazine

비트코인은 프로그래밍 가능한 스마트 머니로, 물수될 수 없고 저축하기에 적합한 모든 특성을 갖추고 있으며 빠른 거래를 원하는 상인들에게도 편리한 결제 수단입니다.

비트코인은 투명한 디지털 원장(ledger)이기 때문에 사기를 감지하고 금융 서비스의 리스크를 분석하는 데 매우 효과가 있습니다. 비트코인은 금과 같은 희소성을 갖고 있는 동시에, 명목화폐 분할성과 휴대성 같은 장점도 제공합니다. 또한 디지털 세계에서 잘 작동하는 새로운 기능들을 도입하고 있습니다.

여러분은 어떻게 생각하나요? 비트코인은 아직 널리 인정받거나 채택되지 않았습니다. 하지만 건전화폐입니까?

제 6장

체험 활동: 수업 토론 - 비트코인은 건전화폐인가?

이제 비트코인에 대해 더욱 자세히 논의했으므로 2장에서 살펴본 화폐의 비교 표를 다시 확인하며 비트코인이 다른 형태의 화폐와 어떻게 다른지 살펴보겠습니다.

좋은 돈의 조건	 소	 담배	 보석	 유로	 비트코인
내구성					
휴대성					
균일성					
수용성					
희소성					
분할 가능성					
총 합					

6.2.3 책임과 권한을 이해하기

“

단일 실패점(single point of failure)이 없는 분산 시스템이 탄생했습니다.
사람들은 개인키를 직접 보유하며, 개인 대 개인 네트워크의 도움을 받아
이중 지불 여부를 확인하고 서로 간 거래를 할 수 있습니다.

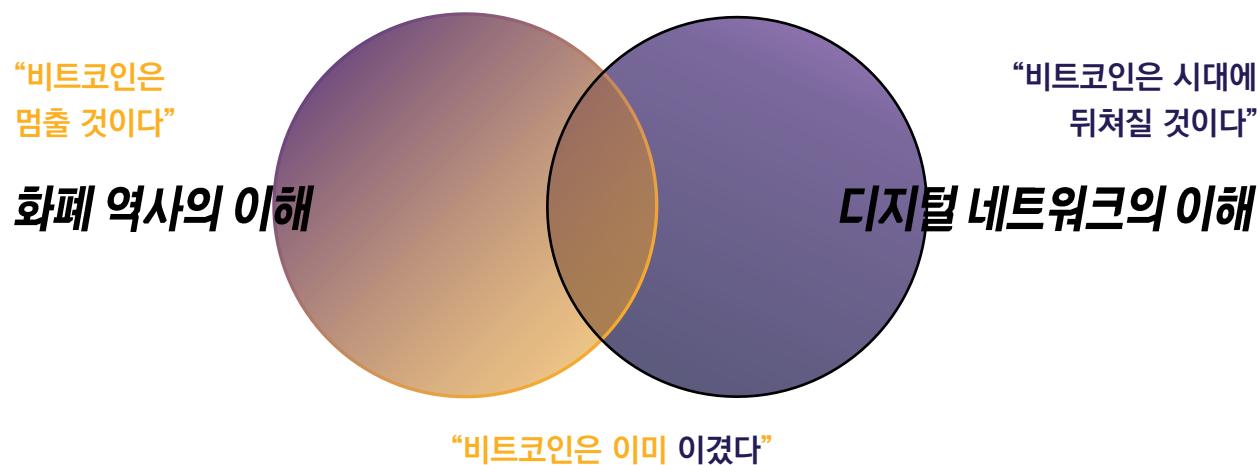
사토시 나카모토

”

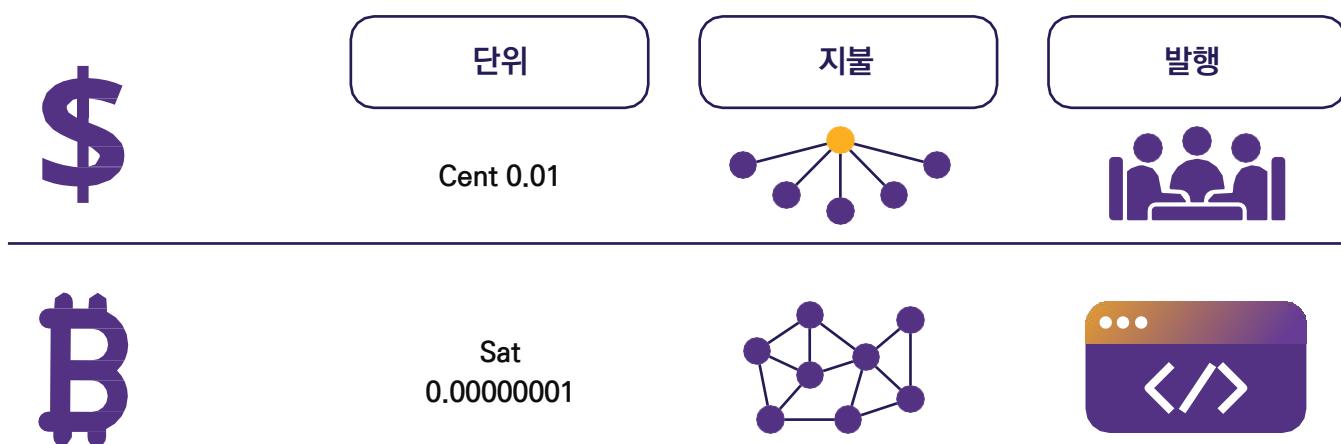
비트코인 소개

명목화폐에서는 사람들이 정부, 은행, 그리고 기존 결제 제공업체에 의존합니다. 이러한 기관 결정권자들이 네트워크의 규칙을 설정하며, 모두가 이 규칙을 따라야 합니다. 여러분이 어디에 살든, 항상 해야 할 일과 정해진 절차가 마련되어 있습니다. 특히 시간이 지남에 따라 많은 가정에 어려움이 그치지 않게 되었습니다.

사람들은 이러한 시스템 때문에 금융 주권을 다른 사람에게 맡기는 것에 익숙해졌습니다. 예를 들어 대부분의 사람들은 문제가 생겼을 때(예: 은행 계좌에 접근할 수 없게 되는 경우) 다른 누군가의 도움에 의존합니다.



비트코인 화폐 시스템은 매우 다릅니다. 비트코인은 독특한 방식으로 작동하며, 명목화폐의 기존 통치자는 규칙이 정해진 시스템으로 대체되었습니다. 비트코인에는 독재자나 지도자가 존재하지 않으며, 그 누구도 여러분에게 무엇을 해야 하는지 강요하지 않습니다. 비트코인이 제공하는 새로운 자유와 권한을 누리고 싶다면, 비트코인 작동 원리를 배우고 자신에게 적합한 방식으로 기술을 이해해야 합니다.





제 6장

비트코인을 쓰면 자금을 완전히 통제할 수 있지만, 그만큼 큰 책임이 따릅니다. 예를 들어, 개인키를 분실하면 비트코인을 영원히 쓸 수 없습니다. 은행처럼 고객센터나 도움을 요청할 수 있는 기관이 없기에 문제가 생기면 스스로 해결해야 합니다.

하지만 삶을 스스로 책임지기로 한 사람들에게는 이런 일이 생기지 않습니다. 비트코인을 쓰는 건 원래 어렵지 않으며, 단지 새로운 개념이라 어렵게 느껴질 뿐입니다. 비트코인이 낯설기에 처음에는 불편하겠지만, 비트코인을 다루는 방법을 배우고, 자신이 직접 책임지는 것을 받아들인다면, 비트코인은 강력한 도구가 됩니다. 여러분이 본인 자금을 온전히 통제할 수 있으며, 아무도 여러분 재산을 빼앗을 수 없습니다.

핵심을 요약하자면, 모든 것을 직접 하는 것입니다. 비트코인 작동 원리를 이해하고, 삶에 맞는 철학으로 적용하는 것이 중요합니다. 다음 장에서는 비트코인 지갑을 설정하고, 거래를 보내고 받으며, 안전한 보안을 설정하는 과정을 시작하겠습니다.

제 7장

비트코인 사용법

7.0 서론

7.1 비트코인 획득 및 교환

7.1.1 P2P: 오프라인 거래

7.1.2 P2P: 온라인 거래

7.1.3 중앙화 거래소

7.2 비트코인 지갑 소개

7.2.1 셀프커스터디 지갑 vs 수탁형 지갑

7.2.2 비트코인 지갑의 종류

7.2.3 오픈 소스 vs 비공개 소스

체험 활동: 수업 토론 - 비트코인 지갑

7.3 모바일 비트코인 지갑 설정

체험 활동: 비트코인 지갑 설정/복구하기

7.4 비트코인 보내기와 받기

체험 활동: 실시간 비트코인 거래 체험

7.5 비트코인 저축

7.4 믿지 말고 검증하라

학습 워크북

한국어 버전 | 2025

비트코인 사용법

7.0 서론

“

사람들은 왜 중앙은행이 아니라 괴짜들의 돈(Nerd Money)을 신뢰할까요?
괴짜들은 인터넷을 만들었고, 은행들은 대공황을 초래했습니다

안드레아스 M. 안토노풀로스

”

이전 장에서 비트코인이 무엇이며, 목적이 무엇인지에 대해 더 깊이 이해하게 되었습니다. 이제는 실제로 사용하는 방법을 배울 차례입니다. 이번 장에서는 비트코인을 획득하는 과정을 단계별로 안내하고, 다양한 종류의 비트코인 지갑, 개인 지갑 설정 방법, 그리고 비트코인 거래를 전송하고 추적하는 실습까지 진행할 것입니다. 이제 이해를 실천으로 옮길 시간입니다!

7.1 비트코인 획득 및 교환

비트코인을 획득하는 방법은 다양합니다.

- ◆ 비트코인으로 급여를 받고, 다양한 제품 및 서비스를
비트코인으로 결제하기 (자세한 내용은 8장에서 다룹니다.)
- ◆ 비트코인을 직접 채굴하기 (자세한 내용은 9장에서 다릅니다.)
- ◆ 명목화폐를 비트코인으로 교환하거나, 비트코인을
명목화폐로 교환하기 (대면거래)
- ◆ 온라인에서 명목화폐를 비트코인으로 교환하거나,
비트코인을 명목화폐로 교환하기



명목화폐를 비트코인으로 교환하는 방법과 대면 거래(P2P) 및 온라인 거래를 통해 살펴보겠습니다.

7.1.1 P2P: 개인

P2P(개인 간) 거래를 통해 비트코인을 획득하거나 판매하는 것은
명목화폐를 비트코인과 교환하는 과정을 포함하며, 은행이나 제3자의 개입
없이 거래를 진행할 수 있습니다.

두 거래 당사자는 교환 금액과 환율을 상호 합의하여 결정합니다. 구매자는
현금을 제공하고, 판매자는 비트코인을 전송하면 거래가 완료됩니다. P2P는
직접 만나 거래하는 것이 더 쉽지만, 온라인 상에서 전 세계 어디서나
원격으로도 거래할 수 있습니다.



7.1.2 P2P: 온라인

P2P(개인 간) 플랫폼은 비트코인 구매자와 판매자가 중개자 없이 인터넷을 통해 거래를 하는 곳입니다.

이러한 플랫폼을 이용하면 개인 정보나 자금을 타인에게 맡길 필요 없이, 다른 사용자들과 직접 만나 비트코인을 사고팔 수 있습니다.



P2P 플랫폼에서는 사용자들이 일정 금액을 에스크로(escrow)로 맡겨, 각자의 거래를 이행하도록 보장해야 합니다. 에스크로(Escrow)란, 거래 당사자들이 합의한 조건을 충족할 때까지, 자금을 안전하게 보관하는 시스템을 의미합니다. 마치 신뢰할 수 있는 친구가 물건을 보관하고 있다가, 서로 약속을 지키면 넘겨주는 것과 같은 방식입니다. (해외 기준이며, 한국에서 에스크로 서비스를 수행하기 위해서는 가상자산사업자가 필요할 수 있습니다.)

7.1.3 중앙화 거래소

중앙화된 거래소는 비트코인을 사는 사람과 파는 사람을 모아서 한번에 연결해주는 플랫폼입니다. 중앙화된 거래소를 이용하는 것은 비트코인을 사고파는 가장 쉬운 방법일 수 있지만 트레이드오프(trade-off)가 존재합니다.



중앙화 거래소와 그에 따른 트레이드-오프

중앙화 거래소를 통해 비트코인을 구매할 때 개인 정보를 제공하고 신원을 인증해야 한다는 점을 유의해야 합니다. 이때 신원 도용 위험을 증가시키고 잠재 보안 위협에 노출될 가능성을 높아집니다. 또한, 중앙화 거래소는 사용자의 비트코인을 보관하므로 출금하기 전까지는 자신의 비트코인을 완전히 통제할 수 없습니다.

심지어 일부 중앙화 거래소는 사용자들의 자금을 유용하거나, 보유한 비트코인보다 더 많은 양을 출금해주다가 결국 파산하기도 합니다. 그러나 비트코인 세계에는 중앙은행이 존재하지 않으며, 사기 행위를 한 거래소를 살리기 위해 화폐를 더 찍어내는 구제 금융(bailout)도 없습니다. 왜냐하면 비트코인은 추가로 발행될 수 없기 때문입니다.

비트코인 사용법

7.2 비트코인 지갑 소개

비트코인은 현금과 달리 실제로 비트코인 지갑(wallet) 안에 존재하지 않습니다. 비트코인은 비트코인 네트워크가 지속 검증하고 보호하는 분산 원장상에 기록되어 있습니다. 그렇다면, 비트코인을 소유하는 방법은 무엇일까요?

비트코인을 소유하려면 거래하고, 소유권을 이전할 수 있는 “개인키(private key)”를 직접 보유하고 있어야 합니다. 즉, 개인키를 통해 거래에 서명하고 비트코인을 전송할 수 있어야 합니다.



이제 “지갑”이라는 개념을 사용할 때 설명하는 두 가지 요소를 살펴보겠습니다.

- ✿ 마스터 개인키(Master Private Key)는 비밀번호와 같은 역할을 하며, 공개키(Public Key)를 생성할 수 있습니다. 공개키는 다른 사람과 공유하여 비트코인을 보내고 받는데 사용됩니다.
- ✿ 모바일 또는 데스크톱 인터페이스: 비트코인 네트워크와 상호작용할 수 있는 플랫폼입니다. 비트코인 잔액을 조회하고, 거래를 주고 받으며, 네트워크에 전파할 수 있습니다.

7.2.1 셀프커스터디 지갑 vs 커스터디 지갑

비트코인 지갑의 다양한 유형과 그 특징을 살펴보기 전에, 아래 표에서 볼 수 있듯이 셀프 커스터디 지갑과 커스터디 지갑 간 차이를 구분하는 것이 중요합니다. 각 유형별 지갑 사용의 장점과 위험성, 그리고 누가 비트코인을 통제하는지를 확인할 수 있습니다. 셀프 커스터디(Self-Custodial)란 사용자가 개인키(private keys)를 직접 보유하는 것을 의미하며 비트코인을 실제로 소유합니다. 반면, 커스터디(Custodial) 지갑에서는 제3자가 사용자 비트코인을 보관합니다.

지갑유형	지갑 통제 권한	장점	위험요소
셀프 커스터디 (자기보관)	사용자	<ul style="list-style-type: none">• 자금과 거래의 완전한 통제권 보유.• 승인 절차 없음, 계좌 동결 없음.• 기업이나 정부 통제를 받지 않음.• 자금 압류로부터 보호되며 집에 돈을 보관하는 것과 유사.	<ul style="list-style-type: none">• 복구 구문(Recovery Phrase)를 분실하면 복구 불가.• 고객 지원 없음.• 사용자에 모든 책임 존재.
커스터디 (수탁)	서비스 제공업체	<ul style="list-style-type: none">• 접근을 잃었을 때 복구가 용이.• 고객 지원 존재.	<ul style="list-style-type: none">• 항상 인터넷에 연결되어 있어 해킹 및 보안 침해 위험 존재.• 제3자가 자금을 통제하며 계좌를 동결할 수 있음.

제 7장

셀프 커스터디 지갑은 사용자만이 개인키를 보유하며, 비트코인의 입출금을 완전히 스스로 통제할 수 있습니다. 반면, 커스터디 지갑은 제3자가 개인키를 보유하며, 사용자를 대신해 해당 지갑의 모든 비트코인을 이동시킬 수 있는 완전한 접근 권한을 갖게 됩니다.

- ◆ 셀프 커스터디 나만의 은행을 운영하는 것과 같습니다. 어떠한 정부나 기업 통제도 받지 않고 자유롭게 거래할 수 있지만, 동시에 비트코인의 보안을 스스로 책임져야 한다는 의미이기도 합니다.
- ◆ 셀프 커스터디는 사용자 동의 없이 제3자가 비트코인을 압류할 수 없습니다.
- ◆ 불확실한 시기에도 비트코인이 안전하다는 확신을 가질 수 있도록 하여 안정감을 제공합니다.

개인에 맞는 적절한 지갑 유형을 선택하는 것이 중요합니다. 사람들은 때때로 설치하려는 지갑이 셀프 커스터디인지, 커스터디 지갑인지 구분하는 것을 어려워합니다. 아래 표에서는 설치 과정에서 두 지갑 간 차이점을 보여줍니다.

지갑 유형	1단계: 지갑 선택	2단계: 지갑 설치	3단계: 새 지갑 생성	4단계: 시드 구문 보관	5단계: 지갑 사용 시작
셀프 커스터디 (자기보관)	셀프 커스터디 지갑 제공업체 선택	지갑 제공업체의 설치 가이드 따르기	복구 구문과 최소 1개의 개인키 생성	복구 구문을 안전한 장소에 보관	지갑을 사용하여 비트코인 송·수신
커스터디 (수탁)	커스터디 지갑 제공업체 선택	지갑 제공업체의 설치 가이드 따르기	지갑 제공업체에서 계좌 생성	해당 없음, 개인키 는 지갑 제공업체가 보유	지갑을 사용하여 비트코인 송·수신

키를 갖고 있지 않으면 코인을 소유한 것이 아니다(Not your keys, not your coins)라는 말은 비트코인 보유자들 사이에서 널리 사용되는 표현입니다. 비트코인 지갑과 연결된 개인키를 직접 통제하지 못한다면 비트코인을 소유하고 있는 것이 아니라는 의미를 담고 있습니다.



개인키에 접근할 수 있다면, 그 사람이 비트코인 소유권자입니다. 따라서 개인키를 철저히 보호하는 것이 무엇보다 중요합니다. 이 책의 뒷부분에서 개인키를 안전하게 보호하는 몇 가지 방법을 살펴볼 것입니다.

앞으로 다룰 내용에서는 셀프 커스터디 지갑만을 다룰 예정입니다. 즉, 사용자가 개인키를 직접 소유하며, 비트코인을 완전히 통제할 수 있는 방식을 중심으로 설명하겠습니다.

걱정하지 마세요. 만약 복잡해 보이거나 모든 것을 완벽히 이해하지 못하더라도 괜찮습니다. 비트코인을 이해해가는 여정이며, 비트코인을 점점 더 사용하다 보면 자연스럽게 이해하게 될 것입니다.

비트코인 사용법

7.2.2 비트코인 지갑의 종류

비트코인 지갑에서 개인키가 생성되고 저장되는 위치에 따라 다르게 부릅니다. 개인키가 스마트폰에 저장되면 모바일 지갑(Mobile Wallet), 개인키가 보안이 강화된 전용 기기에 저장되면 하드웨어 지갑(Hardware Wallet), 개인키가 종이에만 저장된다면 종이 지갑(Paper Wallet)이라고 합니다.

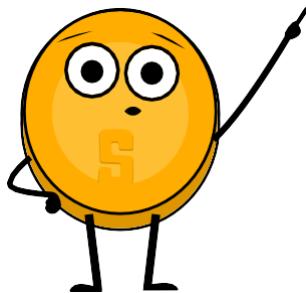
비트코인 지갑 구조에 따른 명칭

지갑유형	설명	장점	단점	추천하는 사용자
온라인 지갑 (Online Wallet)	웹 브라우저를 통해 접근하는 지갑	인터넷 연결이 가능한 모든 기기에서 접근이 가능하여 사용이 간편	보안이 취약하고 해킹 또는 정보 유출 가능성 존재	지갑을 자주 사용하지만 보관할 자금이 많지 않은 사용자
모바일 지갑 (Mobile Wallet)	모바일 기기에 설치된 지갑	편리하며, 스마트폰만 있다면 어디서든 사용 가능	기기를 분실/도난시 자금을 잃을 수 있고, 스마트폰 해킹 가능성 존재	이동 중에도 사용하지만 보관할 자금이 많지 않은 사용자
데스크톱 지갑 (Desktop Wallet)	데스크톱 컴퓨터에 설치된 지갑	온라인 지갑보다 보안성이 높고, 오프라인 사용 가능	컴퓨터가 악성코드에 감염될 경우 해킹 가능성 존재	보관할 자금이 많으며 데스크톱 사용이 편한 사용자
하드웨어 지갑 (Hardware Wallet)	비트코인을 오프라인으로 저장하는 기기	보안성이 매우 높고, 오프라인 사용 가능	하드웨어 지갑 구입 비용 존재	보관할 자금이 많으며 하드웨어 지갑의 추가 보안 비용을 지불할 의향이 있는 사용자
페이퍼 지갑 (Paper Wallet)	비트코인 지갑의 개인키 및 공개키를 기록한 종이 문서	보안성이 매우 높고, 오프라인 사용 가능	종이를 분실하거나 도난당하면 복구 불가능 (자금 손실)	하드웨어 지갑 비용 지불 없이 종이를 인쇄하여 지갑을 만들 의향이 있는 사용자



제 7장

키는 한 기기에서 다른 기기로 이동할 수 있기 때문에, 비트코인 지갑 상태는 고정된 것이 아닙니다. 예를 들어, 컴퓨터에서 비트코인 지갑의 키를 생성한 후 스마트폰에 업로드하면 해당 지갑은 더 이상 데스크톱 지갑이 아닌 모바일 지갑이 됩니다.



비트코인을 저장할 때 중요한 것은 누가 통제하는지 뿐만 아니라 고려해야 할 다양한 요소가 있다는 점입니다. 따라서 보안성과 편의성을 모두 갖춘 저장 방식을 찾거나 나에게 맞는 지갑을 찾는 것이 중요합니다.

비트코인 지갑을 선택할 때 고려해야 할 요소

- ◆ **보안:** 이중 인증(Two-Factor Authentication) 및 안전한 비밀번호 정책과 같은 강력한 보안 기능.
- ◆ **개인정보 보호:** 익명성을 보장하며 계좌 설정을 위한 개인 정보를 요구하지 않는 지갑.
- ◆ **사용 편의성:** 사용이 쉽고 화면 구성이 한눈에 보기 편한 지갑.
- ◆ **호환성:** 지갑이 사용자 기기 및 운영 체제와 호환.
- ◆ **수수료:** 수수료를 직접 설정 가능.
- ◆ **평판:** 해당 지갑과 개발팀의 평판.
- ◆ **통제:** 개인키를 사용자가 직접 통제.

완전한 통제권을 가질 수 있는 지갑이며 조작이 쉽고 편한 지갑인지 확인하며 신중하게 고려하세요.

7.2.3 오픈 소스 vs. 비공개 소스

비트코인 지갑을 선택할 때 중요한 고려사항은 해당 애플리케이션 또는 소프트웨어가 오픈 소스(Open Source)인지 비공개 소스(Closed Source)인지를 확인하는 것입니다. 오픈 소스가 매우 중요한 이유는 비트코인 커뮤니티가 코드를 검토할 수 있고, 만약 개발팀이 개발을 중단하더라도 커뮤니티가 개발을 계속 이어 나갈 수 있기 때문입니다.

비트코인 사용법



비트코인의 코드가 누구나 검토, 사용, 수정할 수 있도록 완전히 공개되어 있는 것처럼, 비트코인을 저장하는 지갑의 코드 또한 공개되어야 합니다.

체험 활동: 비트코인 지갑 토론 및 평가

아래 웹사이트에 접속하세요:

<https://bitcoin.org/en/choose-your-wallet>

오늘 배운 비트코인 지갑의 내용을 기반으로 가장 적합한 지갑을 선택하세요.



7.3 모바일 비트코인 지갑 설정

이제 비트코인 지갑 개념과 차이점을 이해했으므로, 지갑을 설정하고 사용하는 방법을 배워보겠습니다. 이번 예제에서는 스마트폰에서 직접 모바일 지갑을 생성하는 과정을 살펴봅니다.

체험 활동: 비트코인 지갑 설정/복구하기

체험 활동: 옵션 1 – 비트코인 지갑 다운로드

22:03  

비트코인 지갑 생성 및 사용 방법:


Bitcoin wallet
A simple bitcoin wallet for your enjoyment.

[새로운 지갑 만들기](#)

[지갑 불러오기](#)

Your wallet, your coins
100% open-source & open-design

1 앱스토어(iOS) 또는 구글 플레이스토어(Android)에서 앱을 검색합니다.

2 앱을 실행한 후 12개 또는 24개의 복구 구문(시드 구문)을 반드시 적어 안전한 장소에 보관합니다. 이 복구 구문으로 자금을 복구할 수 있습니다.

이 구문들의 순서를 잊어버리거나 잊어버려서 지갑에 접근할 수 없게 될 경우 비트코인을 복구할 수 없습니다.

3 이제 복구 구문(또는 시드 구문)을 실제로 저장했는지 확인해야 합니다. 시드 구문의 단어를 순서로 입력해야 합니다.

4 일부 지갑에서는 안전한 핀 번호(PIN)를 설정할 수 있습니다. 사용자의 개인키(Private Key)와 비트코인 주소는 복구 구문이 자동으로 생성합니다.

공개키(Public Key)를 이메일 주소라고 해보겠습니다. 이메일 주소를 다른 사람과 공유하여 이메일을 받을 수 있듯이, 공개키를 공유하면 다른 사람이 당신에게 비트코인을 보낼 수 있습니다.

개인키(Private Key)는 이메일 비밀번호와 같습니다. 비밀번호를 다른 사람과 공유하면 다른 사람이 이메일에 접속 하듯이, 개인키를 공유하면 다른 사람이 여러분의 비트코인에 접근할 수 있습니다. 따라서 절대 다른 사람에게 공유해서는 안 됩니다.

5 받기(Receive)를 눌러 내 주소로 비트코인을 받습니다. 셀프 커스터디 지갑에서는 명목화폐로 직접 비트코인을 구매할 수 있는 것은 아닙니다. 따라서 거래소에서 비트코인을 구매한 후 지갑으로 전송해야 할 수도 있습니다.

비트코인 사용법

체험 활동: 옵션 2 – 비트코인 지갑 복구하기

22:03

<뒤로

이것은 복구 문구입니다

여기 표시된 대로 반드시 적어주세요.
나중에 이를 확인해야 합니다.

1	gloom	2	police
3	month	4	stamp
5	viable	6	claim
7	hospital	8	heart
9	alcohol	10	off
11	ocean	12	ghost

Backup to iCloud

Print template

검증

비트코인 지갑을 다운로드하고 약간의 사토시를 전송해줍니다.

지갑을 복구할 수 있는 시드 구문(Seed Phrase)이 적힌 용지를 제공해줍니다.

스텝별 안내:

- 기존 지갑 가져오기(Import an existing wallet)를 선택합니다. 그리고 복구 구문으로 복원(Restore with recovery phrase)을 선택합니다.
- 복구 구문 단어 개수에 맞춰 복구 구문을 순서대로 하나씩 입력합니다.
- 입력을 완료한 후 [복원(Restore)]을 누릅니다.
- 지갑이 문제없이 가져와지면 비트코인이 복구됩니다.

7.4 비트코인 보내기와 받기

비트코인 거래란 비트코인의 소유권을 새로운 소유자에게 이전하는 것입니다. 하지만 실제 코인을 전송하는 것이 아니라, 네트워크에 있는 모든 노드가 공용 원장(public ledger) 사본을 업데이트하여 소유권을 변경하는 방식으로 이루어집니다.

비트코인 거래를 보낼 때, 보내는 사람은 자신의 개인키로만 서명할 수 있는 메시지를 생성하여 서명합니다. 이 메시지는 보내는 사람 비트코인의 소유권이 받는 사람으로 변경되었음을 네트워크에 알리는 역할을 합니다.

이제 해당 비트코인은 새로운 소유자만이 전송할 수 있는 주소에 연결되며, 비트코인 소유자가 됩니다.

원장		원장	
소유자	개수	소유자	개수
샘	2.50	샘	2.50
아담	3.00	아담	3.00
마이클	6.00	마이클	6.00
세일러	1.50	세일러▶로라	1.00
로버트	2.00	로버트	2.00
로라	1.75	로라	2.25
다니엘	5.25	다니엘	5.25

새로운 비트코인 거래는 지갑에서 시작되지만, 거래를 처리하는 중앙 결제 처리 기관은 존재하지 않습니다. 대신, 전 세계 채굴자(Miners)들이 거래를 원장에 기록하려고 경쟁합니다.

세일러가 로라에게 0.5 BTC를 빚진 것을 갚으려 한다고 가정해 봅시다.



- 1 로라가 세일러에게 자신의 주소를 공유합니다.
- 2 세일러는 지갑 소프트웨어를 사용하여 로라의 주소, 전송할 금액(0.5 BTC), 채굴자 수수료가 포함된 거래를 생성합니다.
- 3 거래에 서명한 후 네트워크에 브로드캐스트합니다. 네트워크 노드들은 거래를 검증하며, 세일러가 충분한 자금을 보유하고 있는지 확인하는데, 세일러가 충분한 자금이 없다면 거래는 즉시 거부됩니다.
- 4 거래가 검증되면, 채굴자들이 블록에 추가하며 자금이 로라의 주소로 전송됩니다.
- 5 로라는 개인키를 사용하여 전송된 자금을 지갑에서 확인할 수 있습니다.

거래가 완료되면 되돌릴 수 없다는 것을 주의해야 합니다.

비트코인 거래가 작동하는 방법



비트코인 받기



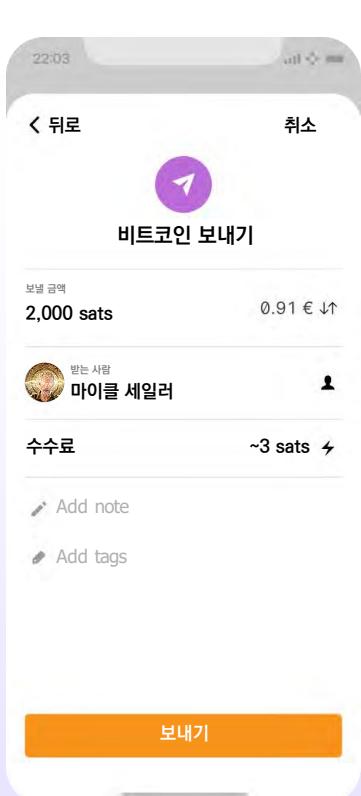
비트코인을 받으려면, 보내는 사람에게 비트코인 지갑 주소를 알려줘야 합니다. 주소는 고유한 문자와 숫자 조합이며, 비트코인 네트워크에서 거래를 인식하는 데 사용됩니다. 비트코인 지갑에 들어가서 “받기(Receive)” 또는 “입금(Deposit)”을 눌러 지갑 주소를 확인할 수 있습니다.

그런 다음, 여러 가지 방법을 통해 보내는 사람과 비트코인 주소를 공유할 수 있습니다.

- 1 주소 복사 및 붙여넣기: 주소를 선택하여 “복사(Copy)”를 눌러 복사한 뒤 이메일이나 메시지에 붙여넣어 보내는 사람에게 전달할 수 있습니다.
- 2 비트코인 지갑 링크 공유: 일부 비트코인 지갑에서는 지갑 링크를 생성하여 공유할 수 있습니다. 보내는 사람이 해당 링크를 클릭하여 비트코인을 전송할 수 있습니다.
- 3 QR 코드 공유: 보내는 사람이 비트코인 지갑 앱이 설치되어 있다면, QR 코드를 스캔하여 비트코인 주소를 가져올 수 있습니다.

비트코인 사용법

보내는 사람이 받는 사람의 전송할 금액을 입력하여 거래를 전송할 수 있습니다. 그리고 비트코인이 지갑으로 전송되며, 거래가 비트코인 네트워크에서 확인되면 지갑에서 확인할 수 있습니다. 이는 보통 몇 분 정도 소요됩니다.



비트코인 보내기

비트코인을 보내려면 비트코인 지갑, 수신자의 비트코인 주소, 그리고 전송할 비트코인 금액이 필요합니다.

- 1 비트코인 지갑을 엽니다. 휴대전화 번호로 전송된 번호를 대화 상자에 입력해야 합니다. 2단계 인증(2FA)을 활성화한 경우, OTP 인증 앱에서 제공하는 6자리 코드를 입력해야 합니다. (2단계 인증이 없는 앱도 있습니다.)
- 2 “보내기(Send)” 또는 “출금(Withdraw)” 기능으로 이동하여 받는 사람 주소를 “받는 사람(To)”에 붙여 넣습니다.
- 3 보낼 비트코인 개수를 “금액(Amount)” 필드에 입력합니다.
- 4 받는 사람의 주소와 전송할 금액이 정확한지 다시 한 번 확인합니다.
- 5 “확인 및 전송(Confirm and Send)”을 누르기 전에 입력한 내용을 다시 한 번 확인하여 올바른 비트코인 금액이 정확한 지갑 주소로 전송되는지 확인하는 것이 좋습니다.
- 6 거래를 확인하고 네트워크에서 거래가 승인될 때까지 기다립니다.

이제 셀프 커스터디 비트코인 지갑을 사용하는 방법을 알게 되었습니다. 비트코인 네트워크에서 한 지갑에서 다른 지갑으로 비트코인을 보내는 것을 “온체인(on-chain)거래”라고 하는데, 메인인 타임체인에서 이루어지기 때문입니다. 온체인 거래는 비트코인을 주고 받는 데 가장 안전한 방법입니다. 그러나 때때로 정산 속도가 느릴 수 있습니다. 8장에서 다룬 라이트닝 네트워크(Lightning Network)거래와 비교하면 속도면에서 차이가 있습니다.

체험 활동: 비트코인 거래 체험

목적: 개인 대 개인 비트코인 거래의 기본 개념과 메커니즘을 이해하는 것.

먼저 비트코인 거래에서 중요한 역할을 하는 주요 참여자를 간단히 정리해 보겠습니다.

- ▶ 보내는 사람과 받는 사람: 서로 비트코인 거래를 원하는 당사자입니다.
- ▶ 노드(Nodes): 거래를 검증하고 타임체인 전체 복사본을 저장하는 역할을 합니다.
라이트 노드(Light Nodes): 저장 공간과 컴퓨팅 자원을 덜 사용하면서도 거래를 검증할 수 있도록 도와줍니다.
- ▶ 채굴자(Miners): 새로운 거래를 타임체인에 추가하는 역할을 담당합니다.

제 7장



각 역할을 이해해야 합니다.

다음 중 하나의 역할이 지정되었습니다: 보내는 사람, 받는 사람, 노드, 채굴자.

- ❶ 보내는 사람: 거래를 생성하고 네트워크에 전송하는 역할을 합니다.
- ❷ 받는 사람: 거래를 받고 검증하는 역할을 합니다.
- ❸ 노드: 거래를 검증하는 역할을 합니다.
- ❹ 채굴자: 거래를 타임체인에 추가하는 역할을 합니다.

노드와 받는 사람 모두 거래를 검증해야 합니다.

❶ 보내는 사람: 거래를 생성합니다.

거래를 생성하려면 다음 단계를 따르세요: 보내려는 코인 개수와 받는 사람의 이름 또는 이니셜을 메모지에 적습니다. 이름이나 이니셜을 서명하여 개인키를 가상으로 서명합니다. 메모지와 보내려는 코인의 개수만큼 받는 사람에게 전달합니다.

❷ 받는 사람: 거래를 검증하는 책임이 있습니다.

- ❶ 메모지를 확인하여 코인 개수와 본인 이름 또는 이니셜이 올바르게 적혀 있는지 확인합니다.
- ❷ 받은 코인의 개수를 세고 메모에 적힌 개수와 비교합니다.
- ❸ 개수가 일치하면 승인란에 기록합니다. 만약 코인이 일치하지 않거나 의심이 든다면 거래를 거부합니다.

보내는 사람 코인	보내는 사람	보내는 사람 서명	받는 사람	날짜 및 시간	받는 사람 승인

❸ 노드로서 맡은 역할: 트랜잭션 검증 및 확인 트랜잭션이 유효한지 확인하는 책임이 있습니다.

- ❶ 보내는 사람의 주소와 받는 사람 주소가 올바른지 검증합니다.
- ❷ 보내는 사람이 충분한 자금을 보유하고 있는지, 해당 거래가 이중으로 지불하지 않았는지 확인합니다.

보내는 사람 코인	보내는 사람	보내는 사람 서명	받는 사람	날짜 및 시간	노드 승인

비트코인 사용법

4 채굴자로서 맡은 역할: 타임체인에 거래 추가합니다.

- 수신자가 승인하고 노드가 검증한 거래를 확인하세요.
- 주사위를 굴려 다른 채굴자 숫자와 비교하세요. 더 작은 숫자가 나온 채굴자가 해당 거래를 타임체인에 추가합니다.
- 시간, 에너지, 노력에 대한 보상으로 포인트를 획득합니다. 가장 많은 포인트를 가진 채굴자가 승리합니다.

**타임체인에 추가된 거래는 변경하거나 되돌릴 수 없습니다.

5 코인 잔액 추적: 활동이 진행되는 동안 디지털 지갑에 있는 코인의 개수를 확인하고 기록하세요.

보낸 코인	보낸 사람	발신자 서명	받는 사람	날짜 및 시간	승인

6 오늘 배운 과정을 토론합니다.

7.5 비트코인 저축

비트코인은 인플레이션에서 여러분의 돈을 보호하고, 누구의 통제 받지 않습니다. 비트코인으로 저축하는 것은 자산을 저장하고, 축적하며, 시간이 지나면서 부를 형성하는 수단이 됩니다.

앞서 배웠듯이, 어떠한 돈을 선택하여 저축할지에 대한 결정은 여러분이 내릴 수 있는 가장 중요한 것 중 하나입니다. 현명한 선택을 하면, 자신과 가족을 위한 더 나은 미래를 만들 수 있습니다.

마음의 평온: 올바르게 보관하면, 비트코인은 누구도 빼앗을 수 없는 유일한 자산입니다.





제 7장

7.6 믿지 말고 검증하라

비트코인을 사용할 때 항상 이 말을 기억해야 합니다. “믿지 말고 검증하라” 비트코인에는 지도자가 없습니다. 누군가의 말을 의심없이 따르는 것은 위험합니다. 그래서 언제나 의심하고 직접 검증해야 합니다. 이 원칙을 따르면 비트코인을 잃지 않고 자신을 보호할 수 있습니다. “제2의 비트코인”, “투자 기회” 또는 “보장된 수익” 등 어떠한 정보도 직접 검증 없이는 받아들이면 안됩니다.

요약. 7장에서 여러분은 일상에서 비트코인을 사용하는 데 필요한 것들을 배웠습니다. 비트코인을 얻고 교환하는 다양한 방법과 보관하는 여러 지갑에 대해 익혔습니다.

모바일 비트코인 지갑을 설정하고 실제 거래를 경험하면서 비트코인을 더욱 자신 있게 사용할 수 있습니다. 또한, 비트코인을 저축하는 방법을 이해하고, “믿지 말고 검증하라”는 원칙을 따름으로써 여러분이 스스로 돈을 통제할 수 있습니다.

다음 장에서는 라이트닝 네트워크를 살펴보겠습니다. 이 새로운 기술이 전 세계 사람들이 돈을 얻고 쓰는 것 방식을 바꾸는 것을 배울 것입니다. 라이트닝 네트워크 일상 거래부터 고급 기능까지 알아보며 개인, 사회, 기업이 어떤 식으로 이용하는지 알아보겠습니다.

제 8장

라이트닝 네트워크: 일상에서 비트코인 사용하기

8.0 서론

체험 활동: 라이트닝 네트워크 설명 영상 시청하기

8.1 라이트닝 네트워크

8.2 라이트닝 지갑 종류

8.2.1 셀프커스터디 지갑 vs 수탁형 지갑

8.2.2 오픈 소스 vs 비공개 소스

8.3 라이트닝 지갑 설정

8.4 라이트닝 보내기와 받기

체험 활동: 라이트닝 릴레이 레이스

8.5 비트코인으로 커피 마시기, 물건 구매하기

8.5.1 온라인: 결제 플러그인 – 전자상거래

8.5.2 오프라인: 주변의 결제매장 찾기

8.5.3 기타 전송방법: 상품권, 기프트 카드 및 직불 카드

8.5.4 지속 가능한 생태계와 교환 매체로서 비트코인

학습 워크북

한국어 버전 | 2025

라이트닝 네트워크: 일상에서 비트코인 사용하기

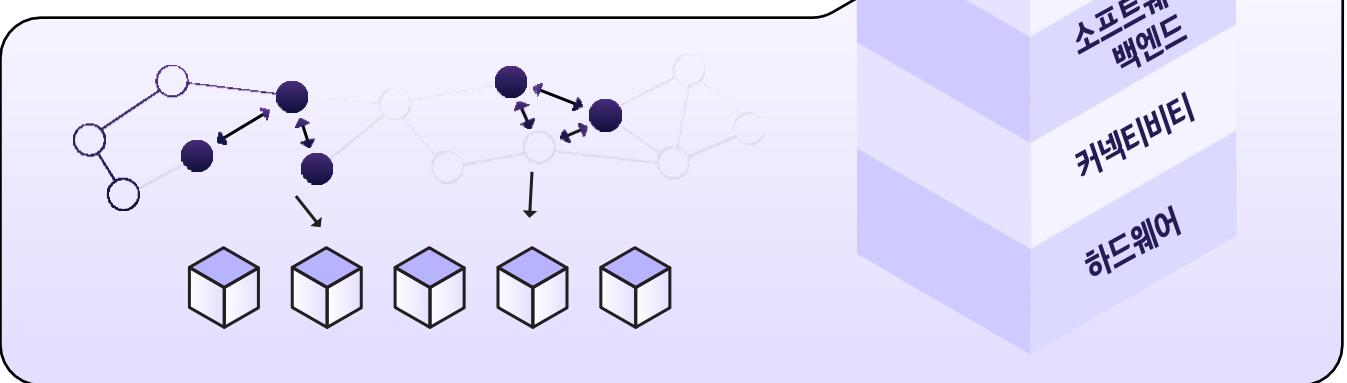
8.0 서론

“우리는 비트코인을 위한 비자(Visa) 네트워크를 구축하고 있습니다.
하지만 비자와 달리, 누구나 그 위에 구축할 수 있다는 점이 장점이라고 생각합니다.”

엘리자베스 스타크

기술은 보통 층층이 쌓이는 방식으로 성장하고 확장됩니다. 예를 들어, 웹사이트, 이메일, 또는 소셜 미디어를 생각해 봅니다. 이것들은 인터넷 프로토콜 위에 구축되었고, 인터넷 프로토콜은 컴퓨터 위에 구축되었으며, 컴퓨터는 전기 위에 만들어졌습니다. 기술들은 처음에는 단순한 설계로 시작하여 시간이 지나면서 계속 발전해 왔습니다.

비트코인도 예외가 아닙니다. 비트코인은 돈의 인터넷이라고 안드레아스 안토노풀로스가 말했듯이 비트코인은 디지털 화폐 기반으로 새로운 기술이 그 위에 쌓일 수 있도록 탄탄한 기초를 제공합니다.



사토시(Satoshi)는 비트코인의 가장 작은 단위입니다. 1달러가 센트로 나뉘듯이, 1비트코인(BTC)은 더 작은 단위인 사토시(SAT)로 나눌 수 있습니다. 1비트코인은 1억 사토시(100,000,000 Sats)와 같습니다.

이 장에서는 라이트닝 네트워크를 통해 비트코인을 전송하는 것을 사토시 보내기(Sending Sats)라고 부를 것입니다. 여기서 “Sats”는 비트코인의 작은 부분(단위)을 의미합니다.

Sats	Bitcoin
1	0.00000001
10	0.00000001
100	0.00000001
1,000	0.00000001
10,000	0.00000001
100,000	0.00000001
1,000,000	0.00000001
10,000,000	0.00000001
100,000,000	0.00000001

체험 활동: 라이트닝 네트워크 영상 시청

라이트닝 네트워크가 작동하는 원리를 다음 영상으로 알아보겠습니다.



8.1 라이트닝 네트워크

라이트닝 네트워크는 비트코인 거래를 빠르고 저렴한 비용으로 처리하는 결제 시스템입니다. 이 시스템은 양측이 일정량의 비트코인을 보유하는 공동 지갑(shared wallet)을 설정하여 작동합니다. 이를 통해, 모든 거래를 메인 원장에 기록할 필요 없이 수 차례 거래를 주고받을 수 있습니다. 그리고 모든 거래가 완료되면 최종 잔액만 원장에 기록합니다.



라이트닝 네트워크는 비트코인을 이용해 빠르고 저렴하게 결제할 수 있도록 하는 결제 시스템입니다. 이 시스템은 두 사람이 공동 지갑(shared wallet)을 설정하여 각자 비트코인을 보관한 뒤, 타임체인을 직접 건드리지 않고 무제한으로 서로 거래할 수 있도록 작동합니다. 모든 거래가 끝난 후, 최종 잔액만 타임체인에 기록됩니다.

카페에서 하루 동안 일을 한다고 미리 일정 금액을 선결제하고 커피를 주문 할 때마다 영수증에 기록만 합니다. 카페에서 일을 다 마치고 떠날 때, 주문한 영수증을 확인하여 최종 금액을 정산합니다. 만약 처음에 선결제한 금액이 최종 금액보다 많다면, 사용하지 않은 금액을 되돌려 받게 됩니다.

이제 수천 명이 이와 같은 방식으로 동시에 결제하고 서로 간 영수증을 활용하여 더 많은 사람들과 연결 되는데, 이것이 바로 라이트닝 네트워크입니다.

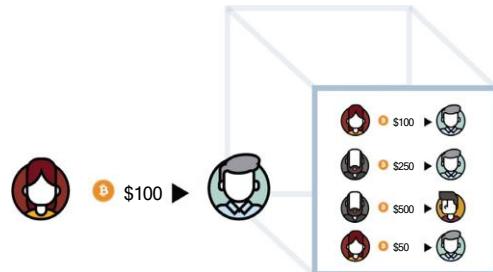
라이트닝 네트워크를 사용하면 누구에게든 비트코인을 보낼 수 있습니다. 비록 받는 사람과 채널이 직접 연결되어 있지 않더라도, 비트코인이 라이트닝 네트워크를 따라 최종 목적지까지 안전하게 전달될 수 있습니다.

이제, 온체인(on-chain) 거래와 오프체인(off-chain) 거래(라이트닝 네트워크)를 비교해 보겠습니다.

라이트닝 네트워크: 일상에서 비트코인 사용하기

온체인(on-chain) 거래:

이 거래는 비트코인 타임체인에서 직접 이루어집니다.
확인하는 데 약 10분이 소요되며, 전송 수수료는 거래
바이트 크기에 따라 달라집니다. 보안성이 높지만 정산
속도는 다소 느린 편입니다.

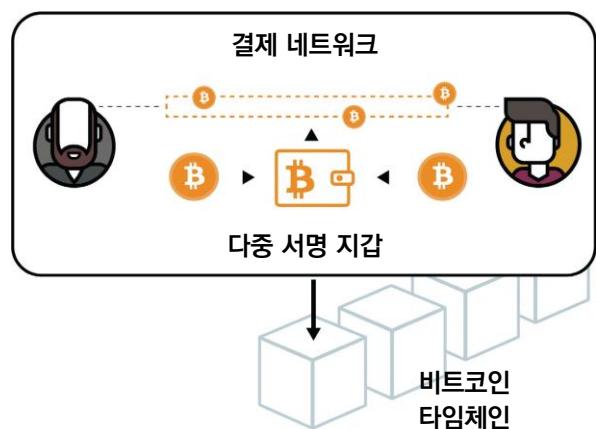


오프 체인(off-chain)거래:

(라이트닝 네트워크)

이 거래는 비트코인 타임체인 위에 구축된 별도의
네트워크에서 이루어집니다. 더 빠르게 처리되며
수수료도 낮습니다.

보통 정산 속도와 비용이 필요한 상황에서 활용됩니다.
온체인 거래와 비교했을 때 보안성이 다소 낮은
편입니다.



지불 네트워크	비트코인 네트워크	라이트닝 네트워크
정의	제3자를 제거하기 위해 암호화 기술을 사용하는 탈중앙화 디지털 네트워크.	비트코인 타임체인 위에서 작동하는 결제 프로토콜로, 더 빠르고 저렴한 결제 네트워크.
장점	탈중앙화 및 보안성 보장. 결제 취소나 사기 위험 없음. 익명 사용 가능. 전 세계에서 사용.	더 빠르고 저렴한 거래. 확장성 증가. 오프체인 거래 방식으로 타임체인 과부하 감소.
단점	정산 속도가 상대적으로 느림. 특정 거래에 대해 높은 수수료 발생.	채널 운영자 신뢰가 필요. 아직 테스트중인 기술이며, 널리 채택되지 않음. 채널을 열고 닫을 때 온체인 거래 필요.



제 8장

8.2 라이트닝 지갑 종류

라이트닝 지갑은 비트코인 지갑과 약간 다르지만, 비트코인 지갑처럼 보내고 받는 역할을 수행합니다. 라이트닝 지갑은 비트코인 네트워크 두 번째 계층(layer 2)인 라이트닝 네트워크에서 비트코인을 전송할 수 있도록 해줍니다.

라이트닝 지갑을 선택하기 전에 고려해야 할 여러 가지 특성이 있습니다.

8.2.1 셀프커스터디 지갑 vs 수탁형 지갑

라이트닝 지갑은 다양한 종류로 나눌 수 있지만, 크게는 셀프커스터디 지갑(Self-Custodial)과 수탁형 지갑(Custodial)으로 구분할 수 있습니다.

비트코인 지갑과 마찬가지로, 셀프커스터디 라이트닝 지갑은 사용자가 직접 개인키(private key)를 관리하는 방식입니다. 반면, 수탁형 라이트닝 월렛은 제3자가 개인키를 관리하는 방식입니다.

수탁형 지갑을 사용할 때 사용자의 접근 권한은 주어지지만, 실제로 지갑은 제3자가 통제합니다. 즉, 편리함을 얻는 대신 비트코인 소유권을 포기하는 것입니다.

소액을 사용할 때는 수탁형 월렛도 괜찮을 수 있지만, 라이트닝 네트워크 기술을 충분히 이해하고 큰 금액을 넣어둘 때에는 셀프커스터디 지갑을 사용하는 것이 좋습니다.

이후 내용에서는 셀프커스터디 라이트닝 지갑(Self-Custodial Lightning Wallets)에 대해서만 다룰 것입니다.

8.2.2 오픈 소스 vs 비공개 소스

라이트닝 월렛도 오픈소스(Open Source)와 비공개(Closed Source)으로 나뉠 수 있습니다. 우리는 항상 오픈소스 지갑을 사용하는 것이 좋습니다. 오픈소스 지갑은 코드가 완전히 공개되어 있으며, 커뮤니티에서 코드 신뢰성을 검증할 수 있기 때문입니다.

오픈소스 애플리케이션은 누구나 소프트웨어 개선에 기여할 수 있다는 의미도 있습니다. 또한 사용자들의 더욱 안전하고 좋은 선택지가 될 수 있습니다.

라이트닝 네트워크: 일상에서 비트코인 사용하기

8.3 라이트닝 지갑 설정

셀프커스터디 라이트닝 월렛을 설정하는 방법은 셀프커스터디 온체인 비트코인 지갑을 설정하는 방법과 동일합니다.

체험 활동: 셀프커스터디 라이트닝 지갑 다운로드

비트코인 라이트닝 지갑 생성 및 사용 방법

1 앱 스토어(iOS) 또는 구글 플레이 스토어(Android)에서 앱을 검색합니다.

2 앱을 열고 12개 또는 24개 복구 구문을 입력합니다. 반드시 이 문구를 적어 안전한 장소에 보관합니다.
이 복구 문구는 자금의 전체 접근 권한을 복구하는 데 사용됩니다.

주의: 이 단어 순서를 잊어버리거나 잊어버리면, 지갑에 접근할 수 없고 비트코인을 복구할 수 없습니다.

3 복구 구문을 실제로 저장했는지 확인해야 합니다. 단어들을 동일한 순서로 입력하세요.

4 일부 지갑에서는 보안을 위해 비밀번호를 설정할 수 있습니다. 개인키와 첫 번째 비트코인 주소는 지갑이 자동으로 생성해 줍니다.

5 라이트닝 인보이스 또는 QR 코드를 생성하여 비트코인을 받을 수 있습니다. 모든 라이트닝 지갑에서 명목화폐로 비트코인을 구매할 수 있는 것은 아니므로, 어떤 라이트닝 지갑에서는 비트코인을 거래소에서 먼저 구매 후 전송해야 할 수도 있습니다.

복구 구문

복구 구문은 계좌를 생성하고 복구하는데 사용됩니다.

1 Issue

2 Flame

3 Sample

4 Lyrics

5 Find

6 Vault

7 Scissors

8 Banner

9 Cute

10 Damage

11 Civil

12 Goat

*참고: 만약 여러분이 수탁형 지갑을 사용하고 있다면, 8.3절의 일부 단계를 따를 필요가 없습니다. 개인키를 직접 관리할 수 없어서 위험이 따릅니다.

이제 비트코인 라이트닝 지갑 설정을 완료했으니 라이트닝으로 비트코인을 보내고 받는 방법을 살펴보고, 7장에서 다뤘던 온체인 거래와 어떻게 다른지 비교해 보겠습니다.



제 8장

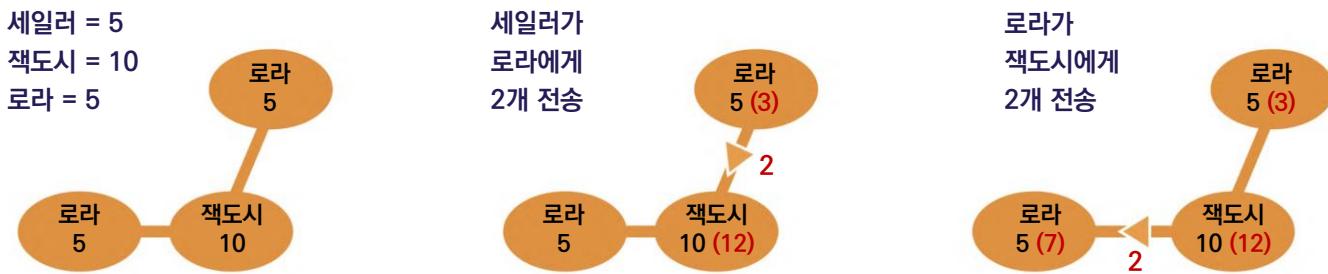
8.4 라이트닝 거래 보내기 및 받기

라이트닝 지갑을 사용하면 비트코인을 빠르고 저렴하게 보낼 수 있어 커피를 사거나 쇼핑을 하는 등 일상 생활에서 쓰기 좋습니다. 라이트닝 네트워크가 작동하는 방법을 알기 위해 몇 가지 예를 살펴보겠습니다.

예시 1:

세일러와 로라는 각각 비트코인 5개가 있습니다. 세일러는 로라에게 2개를 보내고 싶어 합니다. 먼저, 세일러는 잭도시에게 2개를 보냅니다. 잭도시는 다시 로라에게 2개를 전달하면, 로라는 총 7개를 가지게 되며 세일러는 3개를 보유하게 됩니다.

여기서 중요한 점은 세일러와 로라가 은행이나 다른 중개기관을 거치지 않고 거래를 진행할 수 있다는 것입니다.



잭도시는 중개자 역할을 합니다. 세일러와 로라가 서로를 신뢰하지 않는 상황에서, 잭도시는 세일러한테 2개를 받고 로라에게 전달하여 거래를 완료합니다. 잭도시는 라이트닝 네트워크 거래에서 노드 운영자로서, 여러 이점을 누릴 수 있습니다.



전송 수수료

잭도시는 노드를 통해 처리되는 거래마다 소액 수수료를 받습니다. 노드를 유지하고 운영하는 데 들어가는 시간과 노력의 보상입니다.



네트워크 참여

라이트닝 노드를 운영함으로써 네트워크에 참여해 네트워크 탈중앙화, 보안성, 안정성을 높이는 기여를 합니다. 또한 노드 운영자로서 평판과 신뢰도가 상승할 수 있으며, 거래에서 더 경쟁력있는 중개자로 인정받을 수 있습니다.



네트워크 성장

라이트닝 네트워크가 성장하고 더 많은 사람들이 사용하면, 잭도시의 노드를 통과하는 거래 수도 증가할 가능성이 큽니다. 결국 거래 수에 따른 수익 증가로 이어질 수 있습니다.



네트워크 보안 강화

잭도시는 중개자로서 세일러와 로라에게 추가적인 안전망을 제공하여 네트워크 보안을 강화하는 역할을 합니다. 결국 네트워크에 대한 신뢰도를 높아지고, 더 많은 신규 사용자를 유치하게 되어 네트워크 성장에 도움이 됩니다.

라이트닝 네트워크: 일상에서 비트코인 사용하기

예시 2:

로라는 맥도날드를 정말 좋아해서 아침, 점심, 저녁 매일 세끼를 맥도날드에서 먹습니다. 하지만 결제 방법이 너무 많아서 어떤게 가장 좋을지 확신이 서지 않습니다.

로라는 다행히도 비트코인과 라이트닝 네트워크에 대해 배웠습니다. 그리고 아래 표를 비교한 뒤 라이트닝 결제 방식이 가장 좋은 선택이라는 확신을 갖게 되었습니다.

이점	라이트닝 네트워크	기존 금융시스템
정산속도	빠름	느림
투명성	투명	불투명
보안성	안전	취약
거래수수료	낮음	높음
금융 포용성	높음	제한적

이점	라이트닝 네트워크	기존 금융시스템
확장성	높음	낮음
프라이버시	높음	보통
상호운용성	높음	낮음
규제준수	보통	높음
비용 효율성	높음	보통

Visa, Inc.



평균 초당
1,700건의
거래 처리.

최대 초당
65,000건
거래 처리 가능.

비트코인 온체인



최대
초당 7건
거래 처리 가능.

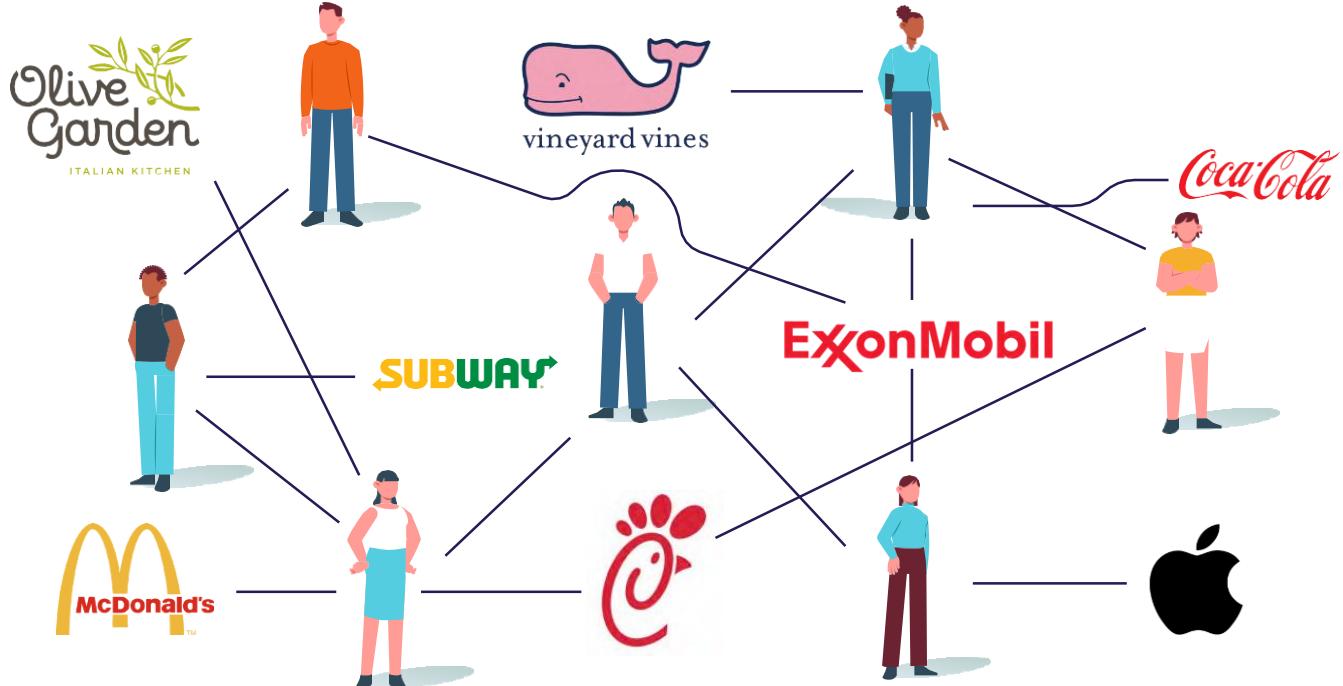
라이트닝 네트워크



초당
수백만 건 거래
처리 가능.

로라는 빠르고 저렴한 거래를 선호하기 때문에, 맥도날드에서 라이트닝 네트워크를 사용해서 결제하기로 결정했습니다. 라이트닝을 사용하면, 정산이 즉시 처리되며 보안성이 뛰어나고 수수료가 저렴하기 때문에 마음 편안하게 식사를 즐길 수 있습니다. 또한, 라이트닝 네트워크는 금융 접근성을 제공하기 때문에, 엘살바도르 외딴 지역에 있더라도 식사 비용을 쉽게 결제할 수 있습니다.

라이트닝을 사용하기 위해, 로라는 먼저 휴대폰에 라이트닝 월렛을 다운로드합니다. 그런 다음, 기존 비트코인 월렛에서 새 라이트닝 월렛으로 비트코인을 전송하여 월렛에 자금을 추가합니다. 이 과정을 "월렛에 자금 추가하기(Funding the wallet)" 또는 "***결제 채널 열기(Funding a payment channel)***"라고 합니다. 로라는 원하는 만큼 비트코인을 라이트닝 월렛에 추가할 수 있지만, 라이트닝 월렛에 잠긴 비트코인은 온체인 거래에서 사용할 수 없다는 점을 유의해야 합니다.



로라의 라이트닝 지갑에 자금이 충전되면, 맥도날드에서 결제를 할 수 있습니다. 맥도날드는 라이트닝 노드를 운영하고 있으므로, 로라는 라이트닝 지갑에서 비트코인을 맥도날드 주소로 보내면서 특정 결제 채널을 열 수 있습니다. 이 과정에서 로라의 비트코인은 비트코인 탐색기에서 라이트닝 네트워크 오프체인 거래로 이동하게 됩니다.

결제 채널이 열려 있을 때 로라는 새로운 채널을 열거나 매번 높은 수수료를 지불할 필요 없이 맥도날드에서 자유롭게 결제할 수 있습니다. 이 채널은 로라와 맥도날드가 계속 사용하기 원할 때까지 유지됩니다. 예를 들어, 로라가 햄버거를 0.0005 비트코인에 구매하면, 채널에서는 로라 잔액이 0.9995 비트코인으로 기록됩니다. 그리고 다음 날 밀크셰이크를 0.0003 비트코인으로 구매하면, 로라의 채널 잔액을 0.9992 비트코인으로 변경하게 됩니다.

라이트닝 네트워크: 일상에서 비트코인 사용하기

로라가 비트코인을 다른 곳에 사용하고 싶을 때에는 채널 종료 거래를 비트코인 타임체인에 브로드캐스트하여 채널을 닫습니다. 로라의 라이트닝 지갑에서 종료 거래를 하면, 로라와 맥도날드가 합의한 채널 최종 잔액이 표시됩니다. 이후 이 거래는 비트코인 타임체인에 브로드캐스트되며 채굴자가 확인합니다. 거래가 확인되면 채널은 닫히고, 채널에 남아 있던 비트코인은 로라와 맥도날드에게 반환됩니다.

채널을 닫는 데는 타임체인에서 확인되는 시간이 걸릴 수 있다는 점을 기억하는 것이 중요합니다. 이 대기 기간 동안 자금은 채널에 잠겨 있어 온체인 거래에 사용할 수 없습니다. 종료 거래가 확인되면 로라는 알림을 받게 됩니다.

이제 라이트닝 지갑을 설정하고 라이트닝 네트워크를 통해 비트코인을 보내는 방법을 배웠으므로, 라이트닝 네트워크를 사용하여 다른 사람들에게 사토시 보내는 게임을 진행할 것입니다.



이것은 라이트닝 네트워크 채널이 연결된 세계 지도입니다. 라이트닝 네트워크를 사용하면 라이트닝 지갑을 가진 사람 누구에게나 사토시를 보낼 수 있습니다. 결제는 몇 초 만에 도착하며, 비용은 단 몇 센트밖에 들지 않습니다.

직접 확인해 보세요.

제 8장



체험 활동: 라이트닝 릴레이 레이스

- 1** 스마트폰이나 컴퓨터에 라이트닝 지갑을 다운로드해야 합니다.
- 2** 챕터 8.3에 나와 있는 내용과 순서에 따라 지갑을 설치합니다.
- 3** 지갑이 설치되면, 열어서 설정을 진행합니다. 새 지갑을 생성하거나 기존 지갑을 복원하는 과정이 포함될 수 있습니다. 또한, 비밀번호나 다른 인증 방식을 사용하여 보안을 강화해야 합니다.
- 4** 비트코인을 받기 위한 라이트닝 송장(invoice), 주소, 또는 QR 코드를 생성합니다.
- 5** 지갑 설정이 완료되고 사토시를 받을 준비가 되면 선생님이 여러분에게 일정량의 사토시를 전송하여 시작할 수 있도록 도와줄 것입니다.



A

목표는 라이트닝 네트워크를 사용하여 여러분 지갑에서 다른 사람의 지갑으로 사토시를 전달하는 것입니다. 그리고 마지막 사람에게 전달 될 때까지 계속합니다.

B

다른 사람에게 사토시를 보내려면, 지갑을 열고 결제를 진행하는 안내를 따르세요. 받는 사람 라이트닝 송장을 제공하거나 QR 코드를 스캔한 후, 보내고 싶은 사토시를 입력해야 합니다.

C

여러분 사토시를 마지막 사람에게 성공적으로 보낸다면 승리합니다.
(그리고 사토시를 그대로 가질 수 있습니다.)

여러분이 체험 활동을 하면서 겪었던 어려움에 대해 이야기해 보세요. 라이트닝 네트워크에서 비트코인을 보내는 것이 쉽고 빠르며 비용이 적게 들었나요? 라이트닝 네트워크가 사용하기 쉽고 이해하기 쉬운 시스템이라고 생각하나요?

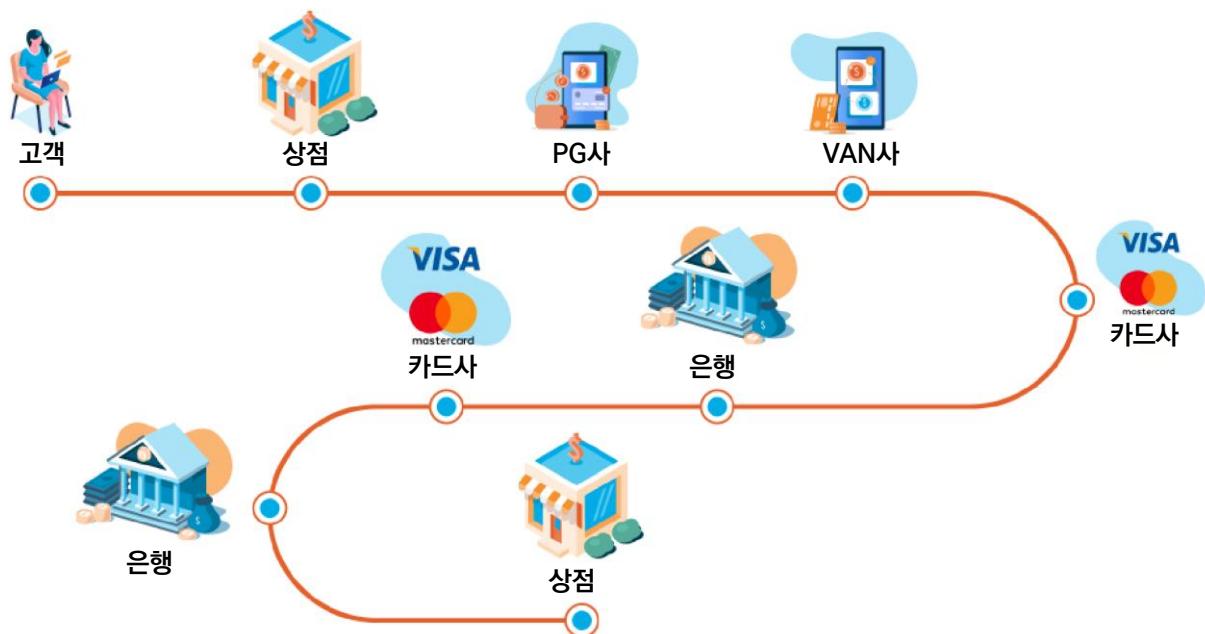
라이트닝 네트워크: 일상에서 비트코인 사용하기

8.5 비트코인으로 커피 마시기, 물건 구매하기

혹시 비트코인을 사용해서 매일 마시는 커피를 사거나 식료품을 살 수 있을지 궁금해한 적이 있나요? 사실 가능합니다. 온라인과 오프라인 모두 비트코인으로 결제할 수 있는 다양한 방법이 있습니다. 우리는 이러한 방법과 도구들을 살펴보며, 비트코인을 사용할 수 있는 상점을 찾는 방법을 알아볼 것입니다.

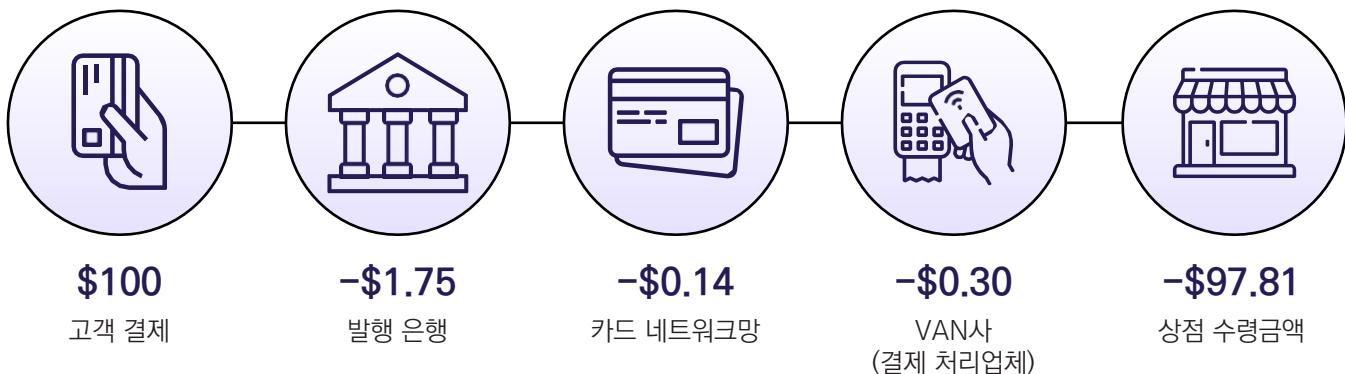
신용카드나 앱으로 결제하는 것이 사용자 입장에서는 간단해 보이지만 실제로 결제 처리는 매우 복잡하며 여러 관련 당사자가 관여합니다.

결제와 지불의 정산 처리과정



물건을 구매할 때 여러 당사자가 관여되며, 각 당사자는 수수료를 부과합니다. 상점 주인에게 이러한 수수료는 상당한 부담이 될 수 있으며, 총 결제 금액의 3% 이상이 될 수도 있습니다. 게다가 여기에 환전 수수료까지 추가될 수도 있습니다.

신용카드 결제 수수료



기업은 비트코인과 라이트닝 네트워크를 통해 국경 없이 인터넷 기반으로 운영되는, 검열에 저항가능한 화폐 시스템으로 전 세계 어디에서든 결제를 즉시 받을 수 있습니다.

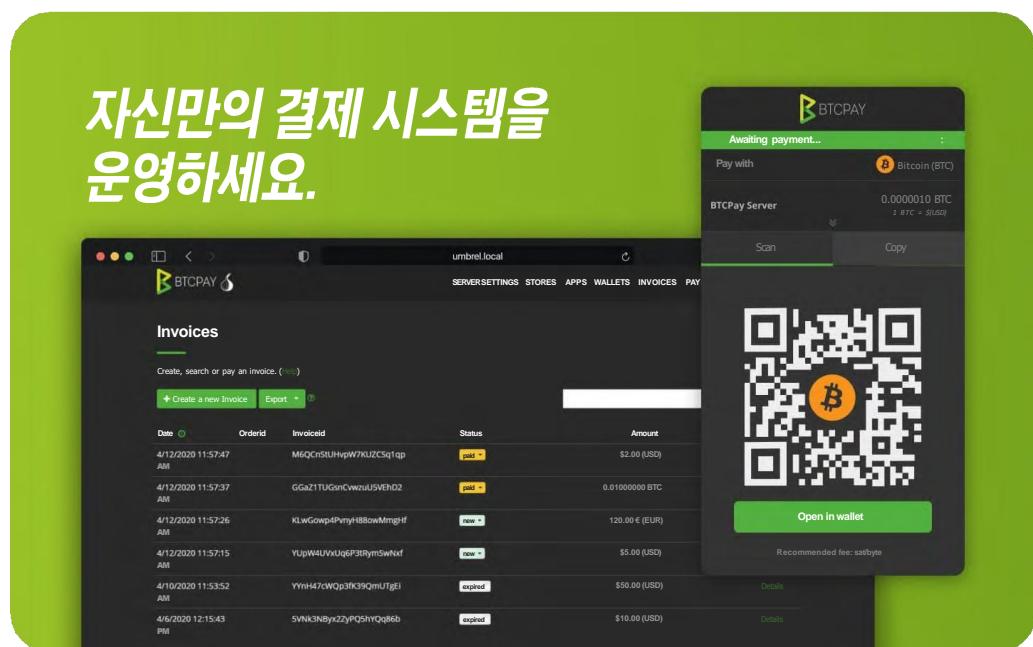
상점들이 비트코인 결제를 쉽게 받을 수 있는 몇 가지 방법을 살펴보겠습니다.

8.5.1 온라인: 결제 플러그인 – 전자상거래

BTCPay Server는 오픈 소스 결제 서비스로, 상점들이 비트코인을 쉽게 받을 수 있도록 도와줍니다. 기술적인 지식이 거의 없어도 사용할 수 있고 무료이며 수수료가 없습니다.

온라인에서 비트코인을 받으려면 BTCPay 플러그인을 웹사이트에 추가하여 BTCPay Server를 간편하게 통합하여 사용할 수 있습니다.

자신만의 결제 시스템을 운영하세요.



라이트닝 네트워크: 일상에서 비트코인 사용하기

BTCPay Server는 기업에서 운영하는 것이 아니고 오픈 소스 프로젝트이기 때문에 컴퓨터 프로그래밍을 익히면 프로젝트에 기여할 수 있습니다.

BTCPay Server에 대해 더 자세히 알아보고, 오프라인 또는 온라인 결제에서 이 시스템을 활용하려면 BTCPay Server 공식 웹사이트를 방문하세요.
(<https://btcpayserver.org>)



8.5.2 오프라인: 주변의 결제매장 찾기

오프라인 매장도 BTCPay Server를 사용하여 비트코인을 받을 수 있으며, 혹은 비트코인 지갑을 다운로드하여 비트코인을 직접 받을 수도 있습니다.



비트코인을 결제 수단으로 받는 상점을 찾으려면 BTCMap.kr에 접속하여 지역을 검색하세요. BTCMap.kr는 비트코인을 받는 상점들이 등록되어 있는 우리나라 지도입니다. 비트코인을 사용하고 싶은 사람들에게 유용한 도구입니다.



8.5.3 기타 전송방법: 상품권, 기프트 카드 및 직불 카드

비트코인을 아직 받지 않는 상점에서 제품이나 서비스를 구매하려면 기프트 카드와 같은 것을 사용할 수 있습니다. 일부 기업은 비트코인과 기프트 카드를 교환하는 서비스를 제공합니다. 비트코인으로 기프트 카드를 구매한 후, 해당 상점에서 직접 사용할 수 있습니다. 비행기 티켓, 호텔, 게임, SIM 카드까지 비트코인으로 거의 모든 것을 구매할 수 있습니다.

8.5.4 지속 가능한 생태계와 교환 매체로서의 비트코인

지속 가능한 생태계(circular economy)란 경제에서 낭비를 최소화하고 가능한 한 많은 제품을 재사용 및 재활용하는 개념에서 비롯되었습니다.

이 개념을 바탕으로 한 비트코인의 지속 가능한 생태계는 비트코인으로 거래가 이루어지고, 비트코인이 경제 내에서 유지되고 성장하여 개인과 기업에 혜택을 주는 경제 시스템을 의미합니다.



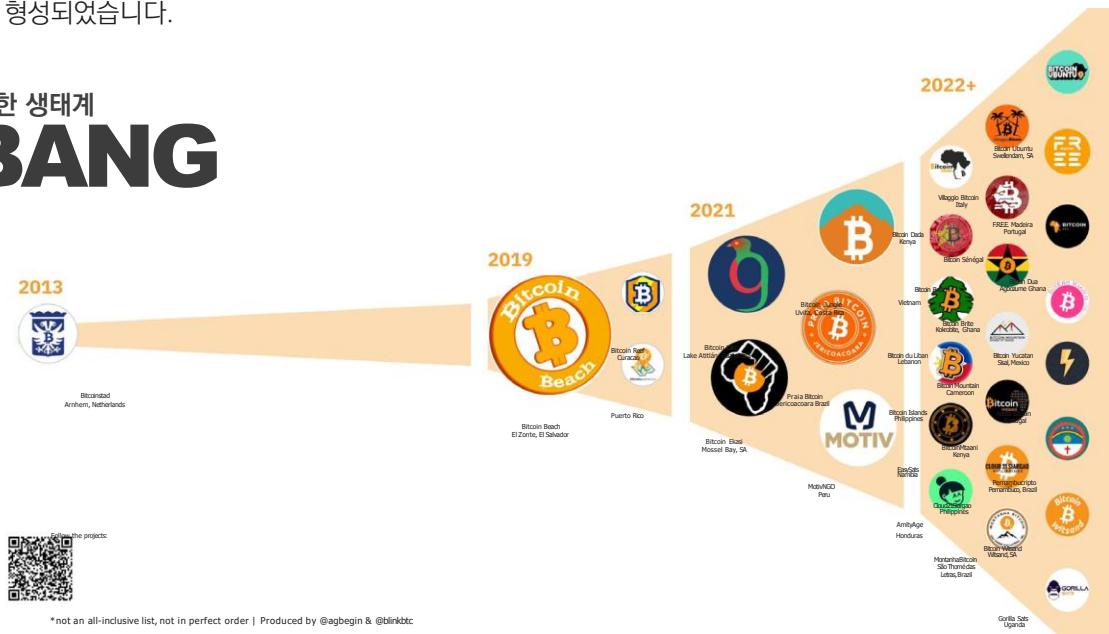
라이트닝 네트워크: 일상에서 비트코인 사용하기

라이트닝 네트워크는 빠르고 저렴한 비트코인 거래가 이루어지며, 전 세계적으로 비트코인의 지속 가능한 생태계가 활성화될 수 있도록 돕습니다.



세계 최초 비트코인 지속 가능한 생태계는 네덜란드 아른헴(Arnhem)에 만들어졌습니다. 이곳은 라이트닝 네트워크가 등장하기 훨씬 이전에 형성되었습니다.

비트코인 지속 가능한 생태계 **BIG BANG**



제 8장

두 번째 비트코인 지속 가능한 생태계 엘살바도르
엘 손테(El Zonte) 비트코인 비치(Bitcoin
Beach)였습니다. 이곳에서는 대부분 은행 계좌가 없던
지역 주민들이 라이트닝 네트워크를 활용하여 즉시
디지털 결제를 할 수 있도록 했습니다.

오늘날 비트코인, 라이트닝 네트워크, 그리고 교육
자료를 기반으로 전 세계에서 수백 개의 지속 가능한
생태계가 형성되고 있습니다



이번 8장에서는 라이트닝 네트워크를 통해 일상생활에서 비트코인을 활용하는 방법을 배웠습니다. 라이트닝 네트워크는 거래를 더욱 빠르고 편리하게 만들어주며, 비트코인이 레이어를 통해 계속 발전하고 변화하는 방식을 미리 경험할 수 있게 해줍니다.

9장에서는 비트코인의 기술적 측면을 탐구할 것입니다. 암호학, 노드, 채굴자 등 비트코인이 실제로 작동하는 원리를 깊이 알아보겠습니다.

제 9장

비트코인 기술 이해

9.0 서론

체험 활동: 비트코인은 작동 원리는 무엇인가? 영상시청

9.1 공개키와 개인키: 암호화를 통한 보안

9.1.1 암호화된 공개키와 개인키

9.1.2 해싱 설명

체험 활동: SHA-256 해시 생성하기

9.2 UTXO 모델

9.3 비트코인 노드와 채굴자에 대한 심층 분석

9.3.1 비트코인 노드란 무엇이며, 어떻게 설정하는가?

체험 활동: 비트코인 노드 영상 시청하기

9.3.2 비트코인 채굴자란 무엇이며, 어떻게 작동하는가?

9.4 메모리풀이란 무엇인가?

체험 활동: 메모리풀

9.5 비트코인 거래의 시작부터 완료까지의 과정

학습 워크북

한국어 버전 | 2025

비트코인 기술 이해

9.0 서론

“비트코인은 “규제되지 않은”것이 아닙니다.
비트코인은 정부가 아닌 알고리즘으로 규제합니다. 변질되지 않습니다.”

안드레아스 M. 안토노풀로스

이번 장에서는 비트코인 네트워크가 완전히 탈중앙화된 방식으로 운영될 수 있도록 하는 기술을 자세히 살펴볼 것입니다. 비트코인을 보낼 때 무슨 일이 일어나며 거래가 처리되는 방법, 그리고 비트코인 네트워크에서 채굴자(Miners)와 노드(Nodes)의 역할이 무엇인지 쉽게 설명할 것입니다. 이번 장에서는 기술 개념들을 다룰 것입니다. 그러나 많은 사람들이 인터넷의 작동 원리를 몰라도 이메일을 보내고, 소셜 미디어로 친구와 연락하고, 온라인 결제를 할 수 있다는 것이 중요합니다. 비트코인이 작동하는 기술과 관련된 것을 배우는 건, 긴 여정이며 비트코인을 화폐로 사용해도 기술을 깊이 이해하지 않아도 됩니다. 우리는 비트코인 기술을 계속 배우는 것을 권장하지만, 이번 장에서는 바탕이 되는 기본 개념에 집중하겠습니다.

비트코인 프로토콜의 작동방식



비트코인의 더 깊은 작동방법 이해를 원한다면, 이 워크북 뒷부분에 포함된 자료를 참고하세요. 또한, 새로운 내용 과정이 준비되었을 때 알림을 받을 수 있도록 우리 웹사이트 비트코인 디플로마 – 기술 편(Bitcoin Diploma – Technical Edition)에 등록할 수도 있습니다.

체험 활동: 비트코인 네트워크 작동방식을 보여주는 영상을 함께 시청하며 알아봅시다.



비트코인 네트워크는 단순히 거래 내역을 저장하는 원장(ledger)이며 이는 노드(nodes)라고 불리는 여러 컴퓨터에 분산되어 저장됩니다. 비트코인 원장은 가명성(pseudonymous)이 있으며 개인 정보 없이, 오직 거래 내역과 주소 정보만 기록됩니다. 이 원장에는 비트코인 네트워크가 시작된 2009년 1월 3일 이후 모든 비트코인 이동 기록이 남아 있습니다.

9.1 공개키와 개인키: 암호화 통한 보안

“

비트코인이 우리에게 제공하는 것은 확실한 약속입니다:
프로그램은 지정된 대로 정확하게 실행됩니다.

안드레아스 M. 안토노풀로스

”

9.1.1 암호화된 공개키와 개인키

암호학(Cryptography)은
정보를 코드로 변환하여 기밀을
유지하는 방법입니다.



 암호화(encryption)는 정보를 특별한 코드로 변환하여,
올바른 해독(decrypt) 방법을 모르는 사람은 읽을 수
없도록 만드는 과정입니다. 마치 금고를 잠그는 것과
같아서, 정확한 열쇠를 가진 사람만 열 수 있는 것과
유사합니다.

 반면, 복호화(decryption)는 암호화된 정보를 다시
읽을 수 있도록 변환하는 과정입니다. 마치 금고를 열어
내부 정보를 읽을 수 있게 하는 것과 같습니다.

예를 들어, 세일러가 로라에게 다른 누구도 읽을 수 없는 비밀
메시지를 보내고 싶다고 가정해 봅시다. 그들은 메시지를
전송하기 전에 피그펜 암호화(Pigpen Cipher)방식을
사용하여 내용을 변환하기로 합의합니다. 이 암호를 알고 있는
사람만이 메시지를 해독할 수 있기 때문에, 다른 사람들은
내용을 읽을 수 없습니다. 비록 이 방법은 오늘날 안전한
암호화 방식으로 간주되지는 않지만, 개인키 암호화(private-
key cryptography)를 이용해 메시지를 보내는 원리를
설명하는 좋은 예시입니다.

피그펜 암호 (Pigpen Cipher)

피그펜 암호를 해독할 때, 플레이어는
**암호화된 메시지와
암호표(cipher)**를 받게 됩니다.
메시지를 복호화하려면, 암호화된
메시지에서 각 기호를 암호표에서 찾아
해당하는 문자로 변환하면 됩니다.

 암호화된 메시지 예:



A	B	C	J	K	L	S	W
D	E	F	M	N	F	T	U
G	H	I	P	Q	R	V	Z

그렇다면 비트코인 거래에서 암호화가 작동하는 원리는 무엇일까요?

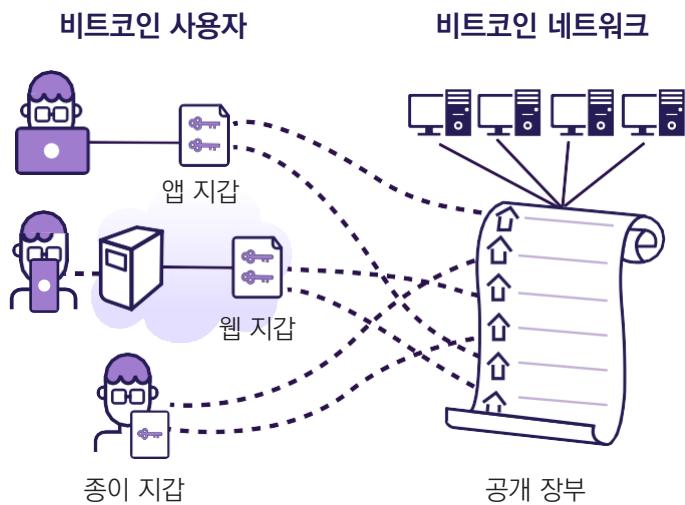
기존 개인키 암호화에서는, 세일러와 로라가 피그펜 암호 같은 개인키를 공유해야 합니다. 세일러는 개인키를 사용하여
메시지를 암호화(encrypt) 한 뒤 로라에게 보냅니다. 로라는 동일한 개인키를 사용하여 메시지를 복호화(decrypt)하고 읽을 수
있습니다. 하지만 제3자가 동일한 개인키를 가지고 있다면 메시지를 가로채어 복호화하고 읽을 수도 있습니다.

비트코인 기술 이해

비트코인 거래에 사용되는 공개키 암호화(Public Key Cryptography)는 이 문제를 해결했습니다. 공개키 암호화에서는 세일러와 로라가 서로 비밀번호나 암호화 방법을 공유할 필요가 없지만 각자 두 개의 다른 키가 있어야 합니다. 하나는 **공개키(Public Key)**로, 아무에게나 공유해도 안전지만, 다른 하나는 **개인키(Private Key)**로 유출해서는 안됩니다.

세일러가 로라에게 메시지를 보내고 싶다면, 로라의 **공개키**를 사용하여 메시지를 암호화한 후 전송할 수 있습니다. 로라가 메시지를 받으면, **개인키**를 사용하여 복호화할 수 있습니다. 제3자가 메시지를 가로채더라도 복호화할 수 없기 때문에, 메시지를 읽을 수 없습니다.

또한, 세일러와 로라가 서로 개인키를 공유할 필요가 없기 때문에, 개인키가 도난당할 가능성도 훨씬 낮아집니다.



따라서 개인키 암호화보다 공개키 암호화가 더 좋은 점은, 보내는 사람과 받는 사람이 개인키(또는 피그펜 암호 같은 암호화 방법)를 보내기 전에 공유할 필요 없이 안전한 통신이 가능하다는 점입니다. 개인키를 사전에 공유해야 한다면 제3자가 가로챌 위험이 있기 때문입니다.

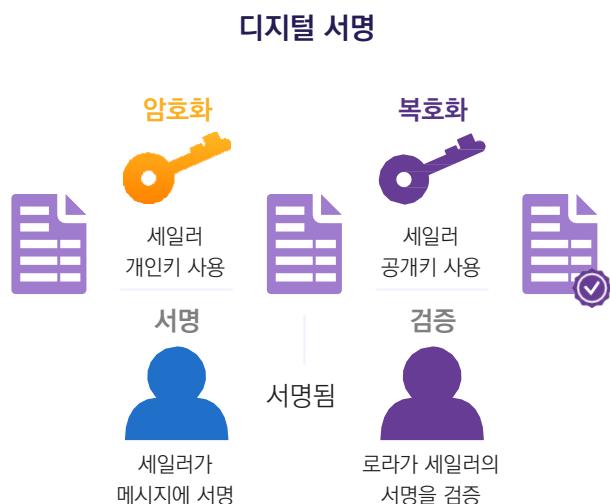
비트코인에서는 공개키 암호화가 암호화된 메시지를 전송하는 용도로는 사용되지 않습니다. 비트코인 거래를 변경할 수 없도록 고유한 **디지털 서명(Digital Signature)**을 생성하는 데 사용됩니다. **디지털 서명**은 비트코인 거래 신뢰성을 증명하는 방식으로, 종이에 서명을 하는 것과 같은 역할을 합니다.

공개키 암호화 (두 사용자 간 모든 거래에서 사용)

각 사용자는 두 개의 키를 가집니다. 하나는 **개인키**로, 유출되지 않게 해야 하고 다른 하나는 **공개키**로, 다른 사람과 공유할 수 있습니다.

개인키는 신원 확인 및 소유권 증명 역할을 하며 주소에 대한 소유권과, 제어할 수 있는 권한이 있다는 사실을 확인해 줍니다.

디지털 서명은 고유한 거래를 식별하기 위해 생성됩니다.

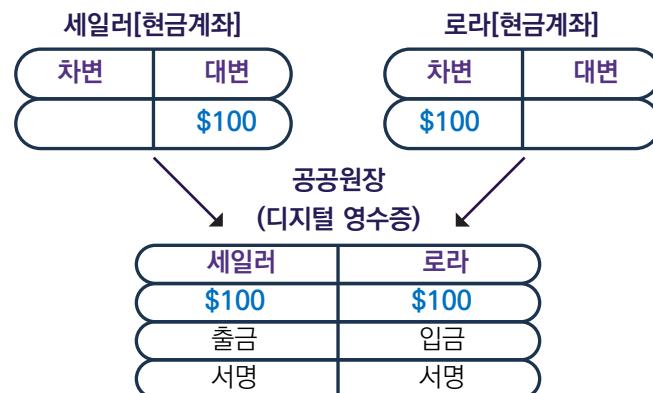


제 9장

비트코인 거래는 비트코인을 다른 사람의 계정으로 직접 전송하는 과정입니다.

암호화 덕분에 비트코인 실제 소유자만이 자금을 다른 사람에게 보낼 수 있으며, 악의를 가진 행위자로부터 안전하게 보호될 수 있습니다.

또한 비트코인에서 보낸 모든 거래는 자동으로 **고유한 서명(UNIQUE signature)**이 존재합니다. 이 서명은 변조 방지 기술(tamper-proof technology)을 활용하여, 비트코인 실제 소유자가 거래를 보냈음을 네트워크가 검증할 수 있도록 합니다. 즉, 제3자가 보내는 것이 아님을 보장합니다.



실제 비트코인 거래가 작동하는 방법을 쉽게 설명합니다:

- 거래 생성:** 사용자가 비트코인 거래를 위해 받는 사람 주소와 전송할 비트코인 개수를 입력합니다.
- 디지털 서명 생성:** 보내는 사람은 **개인키**를 사용하여 고유한 **디지털 서명**을 생성합니다. 이 서명은 거래 신뢰성을 검증하는 암호학 기반의 코드 역할을 합니다.
- 거래 브로드캐스트:** 서명이 완료된 거래는 비트코인 네트워크에 브로드캐스트(전송)되며, 보내는 사람이 비트코인 소유권을 받는 사람에게 이전하려 한다는 신호를 보냅니다.
- 네트워크에서 검증:** 비트코인 네트워크 노드(Nodes)들은 거래를 수신하여 검증합니다. 받는 사람 **공개키**를 사용해 거래의 무결성을 확인하고, 동시에 보낸 사람 **공개키**를 사용해 **디지털 서명**도 검증합니다.
- 비트코인 네트워크에서 확인:** 검증이 성공하면 거래는 타임체인 원장(Ledger)에 기록되며, 이는 모든 거래를 안전하고 투명하게 저장하는 역할을 합니다. 거래가 완전히 확인(Confirmed)되면, 비트코인 소유권이 보낸 사람에서 받는 사람으로 이전됩니다.



즉, 보내는 사람 개인키로 생성된 디지털 서명은 거래 신뢰성과 소유권을 증명하는 암호학 기반의 코드 역할을 하며, 비트코인 탈중앙화 네트워크가 거래를 검증하고 원장에 기록할 수 있도록 합니다.

비트코인 기술 이해

9.1.2 해싱 설명

기술 용어와 수학 개념이 등장하더라도 겁먹지 마세요. 모든 사람이 수학을 좋아하는 것은 아니라는 것을 이해하지만, 노력을 조금만 기울이면 가장 복잡한 개념조차도 이해할 수 있다는 점에서 스스로 놀라게 될지도 모릅니다.

함수(Function)란 무엇일까요?

함수(Function)는 정보를 받아 새로운 것으로 변환하는 기계와 같습니다.

함수에 입력하는 정보를 **입력(input)**이라고 합니다. 함수가 생성하는 새로운 정보는 **출력(output)**이라고 합니다. 함수는 컴퓨터가 작업을 수행하고 문제를 해결하는 데 도움을 줍니다.

이것을 샐러드 레시피로 생각해봅시다. 레시피(또는 함수)는 섞어야 하는 재료와 방법을 알려줍니다. 다른 재료를 넣을 수도 있지만, 레시피대로 만든다면 샐러드가 동일한 결과물로 나오게 됩니다. 함수는 작업을 더 쉽고 효율 있게 수행하는 데 도움을 줍니다.

이 레시피는 함수로 작동하며, 재료를 **입력**으로 받아 샐러드를 **출력**으로 생성합니다.

비트코인에서는 함수를 이용하여 거래를 실행합니다. 거래는 한 주소에서 다른 주소로 돈을 전송하는 과정이며, 거래 위해 여러 암호화 함수(Cryptographic Functions)가 사용됩니다. 암호화 함수는 거래를 검증하며 비트코인 원장 상태를 업데이트합니다.

비트코인 거래에서 사용되는 함수에는 보내는 사람이 충분한 자금이 있는지 확인하며, 거래를 검증하고 주소들의 잔액을 업데이트하는 기능이 포함됩니다. 거래가 검증되고 블록에 추가되면 네트워크상 모든 거래 원장에 언제까지나 남게 됩니다.

단방향 함수(One-Way Function)란?

단방향 함수는 일련의 명령을 사용하여 새로운 것으로 변환하는 함수인데, 스무디를 만들기 위해 여러 재료를 섞어 만드는 것과 같습니다. 하지만 스무디를 만들고 나면 원래 재료로 되돌릴 수 없는 것처럼, 단방향 함수도 한 번 변환된 정보를 다시 원래 상태로 되돌릴 수 없습니다.



공개키 암호화에서 **공개키**는 단방향 함수를 기반으로 하며, **공개키**로 **개인키**를 알아내기 어렵게 만듭니다. 이론에 따르면 **공개키**에서 **개인키**를 찾는 것이 완전히 불가능한 것은 아니지만, 수행하는 것은 극도로 어렵고 엄청난 시간과 연산 능력이 필요합니다.

비트코인에서 **공개키**로부터 **개인키**를 찾는 과정은 축구 경기장 크기의 건초 더미에서 바늘을 찾는 것과 같습니다. 바늘은 **개인키**를 의미하며, 건초 더미는 찾아 볼 수 있는 모든 **개인키**를 의미합니다. 이와 같이 단방향 함수는 되돌릴 수 없도록 설계되어 있으며, 복호화 할 수 없습니다.

해시 함수란 무엇인가?

해싱(Hashing)은 디지털 데이터 지문과 같습니다. 디지털 메시지를 입력받아 고정된 길이의 코드로 변환하는 과정으로, 해당 코드가 고유한 식별자(Unique Identifier) 역할을 합니다.

지문이 사람을 식별할 수 있는 것처럼, 해시는 디지털 메시지를 식별할 수 있습니다. 해시는 비트코인 거래를 포함한 다양한 응용 분야에서 사용됩니다.

비트코인 거래에서 해싱이 사용되는 방법

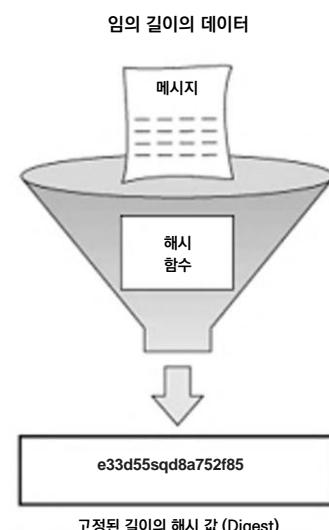
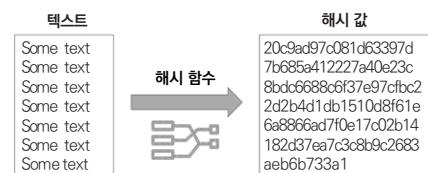
비트코인에서는 모든 거래가 타임체인 원장에 추가되기 전에 해싱됩니다. 해시는 거래 서명(Signature) 역할을 하며, 해당 거래가 유효하고 변조되지 않았음을 확인하는 기능을 합니다. 만약 누군가 거래 내용을 변경하려 하면, 해시 값이 완전히 달라지게 되며, 이를 통해 변경 사항이 감지됩니다.

비트코인 보안에서 해싱의 역할

해싱은 비트코인 네트워크 보안에 반드시 필요한 요소입니다. 해시를 사용하여 거래를 식별함으로써, 네트워크는 거래를 조작하거나 변경하려는 시도를 감지할 수 있습니다. 이것은 사기를 방지하고, 모든 거래가 원장에 정확하게 기록되도록 보장하는 역할을 합니다.

해시 함수는 단방향 함수(One-Way Function) 한 종류로, 입력 값(메시지 또는 데이터)을 받아 숫자로 된 고유한 해시 값(Hash)으로 변환하는 역할을 합니다. **출력된** 해시는 입력 값에 따라 나오는 고유한 값이므로, **입력 값**이 조금이라도 변경되면 완전히 다른 해시 값이 생성됩니다.

해시 함수는 마치 비밀 코드 생성기와 같습니다. **메시지**를 입력하면 코드로 변환합니다.



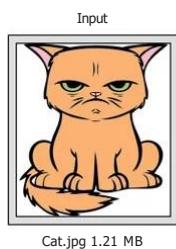
비트코인 기술 이해

같은 메시지에는 항상 동일한 코드가 생성됩니다. 하지만 메시지를 조금이라도 변경하면, 코드는 완전히 달라집니다. 이것은 컴퓨터가 데이터를 기억하고, 변경 사항이 있는지 확인하는 데 도움을 줍니다.



어떤 문자열이나 입력 값이든 즉시 SHA256 해시를 생성할 수 있습니다. 해시 함수는 단방향 방식으로 사용됩니다.

체험 활동: SHA-256 해시 생성하기 →



출력
dee6a5d375827436
ee4b47a930160457
901dce84ff0fac58bf
79ab0edb479561
A 32-byte hash



이전 해시와 완전히 다릅니다.
 출력
d2ca4f53c8257301
86db9ea585075f96
cd6dfbf4fb7c687
a23b912b2b39bf6
A 32-byte hash

출력값, 즉 해시는 원래 입력 길이와 관계없이 항상 동일한 길이를 가집니다.

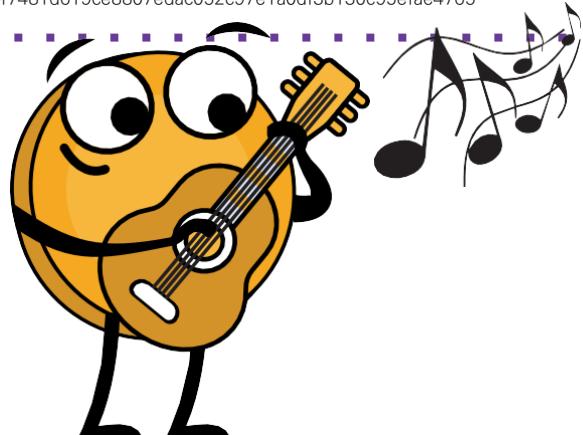
비트코인은 **SHA-256**과 **RIPEMD-160**이라는 특정한 해시 함수를 사용합니다. 아래는 몇 가지 예시입니다.

두 번째 입력에서 작은 변화를 주었을 때, 출력이 완전히 달라진다는 것을 확인할 수 있습니다.

세 번째 입력 길이는 매우 길지만, 출력값은 여전히 다른 두 개와 동일한 고정된 길이를 유지합니다.

- ▶ 문자열 "hello world" SHA-256 해시 값
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- ▶ 문자열 "hello world." SHA-256 해시 값
7ddb227315f423250fc67f3be69c544628dff41752af91c50ae0a9c49faeb87
- ▶ Ubuntu 18.10로 다운로드 가능한 iso 파일의 SHA-256 해시 값
7b9f670c749f797a0f7481d619ce8807edad052c97e1a0df3b130c95efae4765

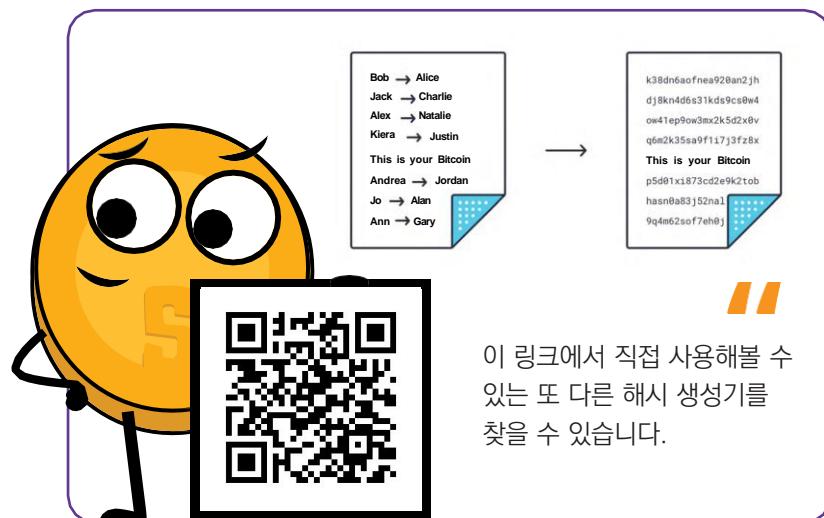
해싱(Hashing)은 음악 악보로 비유할 수 있습니다. 악보가 특정한 곡을 표현하는 것처럼, 해시 값도 특정 데이터를 나타냅니다. 연주자가 악보와 실제 연주를 비교하여 연주의 정확성을 확인할 수 있는 것처럼, 받은 데이터 해시 값을 원래 해시 값과 비교하면 전송 중에 데이터가 변경되었는지 확인할 수 있습니다.



음악 연주에서 조금만 변형되어도 곡의 느낌이 달라지는 것처럼, 원본 데이터에서 아주 조금만 변경되어도 완전히 다른 해시 값이 생성됩니다. 이러한 특성 덕분에 해싱(Hashing)은 비트코인 거래 무결성과 신뢰성을 보장하는 강력한 도구로 활용됩니다.

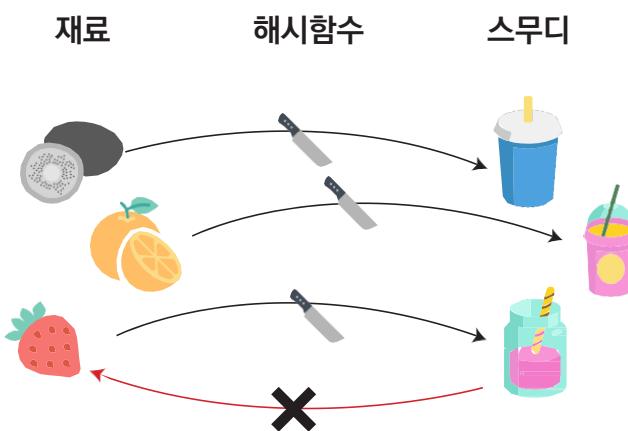
공개키를 해싱하는 과정은 정보를 고정된 길이의 읽을 수 없는 형식으로 변환하여 보안을 강화하는 역할입니다.

비트코인은 SHA-256 및 RIPEMD-160 알고리즘을 사용하여 공개 주소(Public Address)를 생성합니다. 이렇게 생성된 출력 값은 **공개키**의 고유한 식별자 역할을 하며, 원장에 저장된 거래 무결성과 보안을 보장하는 데 도움을 줍니다. 이와 같은 방식으로 정보를 암호화하면, 승인되지 않은 사용자가 데이터를 무단으로 접근하거나 조작하는 것이 더욱 어려워집니다.



해싱(Hashing)

해시 함수는 어떤 입력값이든 받아들여 고정된 길이의 출력값(해시)을 생성합니다.



결정론적(Deterministic)

같은 재료를 사용하면 항상 동일한 스무디가 만들어 진다.



일방향성(Pre-Image Resistance)

스무디가 만들어졌을 때, 딸기를 다시 원래대로 되돌릴 수 없다.



상관관계 저항성(Correlation Resistance)

재료를 조금만 변경해도 완전히 다른 스무디가 만들어진다.



충돌 저항성(Collision Resistance)

서로 다른 재료를 사용하여 완전히 동일한 스무디를 만드는 것은 매우 어렵다.



속도와 검증 가능성(Speed & Verifiability)

과일을 믹서에 넣으면 빠르게 스무디가 만들어지고, 그 결과가 확실하다.

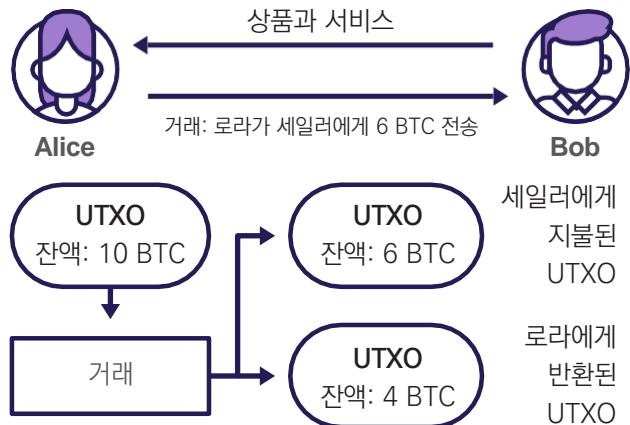
비트코인 기술 이해

9.2 UTXO 모델

UTXO란 무엇인가요?

비트코인에서 거래는 큰 금덩어리를 작은 조각으로 나누어 자신과 다른 사람에게 보내는 방식과 유사하게 작동합니다.

UTXO는 비트코인의 다양한 크기와 조각 또는 지갑 안의 여러 종류의 지폐와 비슷하다고 생각할 수 있습니다. UTXO를 사용할 때, 받는 사람을 위한 새로운 UTXO가 생성되며, 남은 금액은 잔돈(Change UTXO)라는 새로운 형태로 다시 거슬러집니다. 이것은 마치 \$10 지폐로 커피 두 잔을 \$6에 구매하는 것과 같습니다. 커피숍은 \$6을 받고, 남은 \$4를 거스름돈으로 돌려주는 것과 같은 원리입니다.

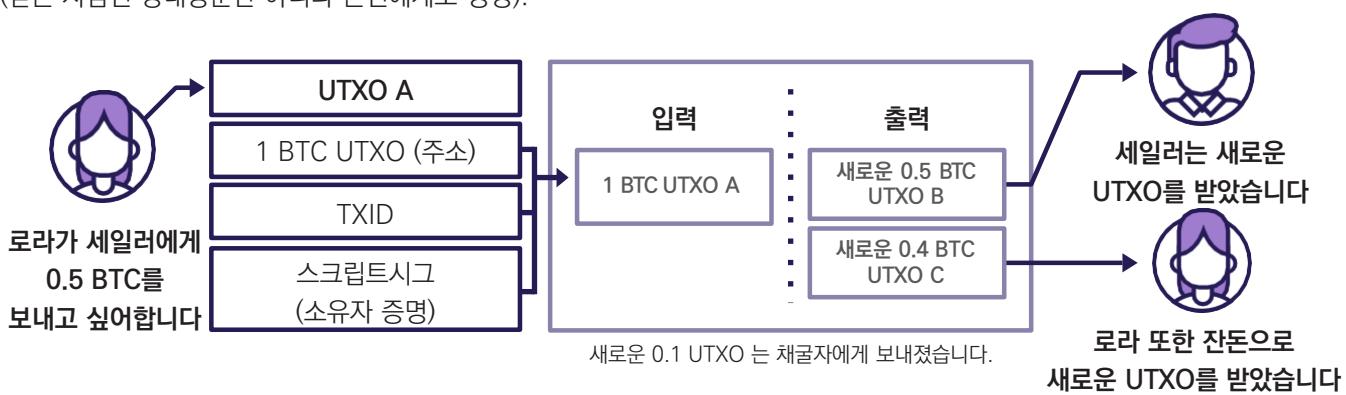


비트코인을 보낼 때, 비트코인 지갑에 있는 UTXO를 전송해야 합니다. 일부는 받는 사람에게 보내지고 남은 금액은 새로운 비트코인 주소에 잔돈(change) 형태로 반환됩니다. 이때 반환된 잔돈은 미사용 트랜잭션 출력(UTXO, Unspent Transaction Output)이라고 하며, 향후 새로운 거래에서 입력값으로 사용할 수 있습니다.

비트코인 지갑의 잔액은 모든 UTXO의 합입니다. 즉, 보유한 모든 UTXO의 총합이 자신의 비트코인 총 보유량이 됩니다.

자신의 UTXO를 다른 사람에게 알리지 않는 것이 중요합니다. 누군가 UTXO를 알게 되면 비트코인 네트워크에서 거래를 추적할 수 있으며, 보유한 비트코인 총액을 파악할 수 있게 됩니다.

결론적으로, 거래를 할 때마다 기존 UTXO를 사용하여 비트코인을 소비하며, 새로운 UTXO가 생성됩니다. (받는 사람인 상대방뿐만 아니라 본인에게도 생성).



거래가 이루어지면, 전송된 비트코인 금액은 여러 개의 출력(Output)으로 나뉘며, 각 출력은 새로운 UTXO와 연결됩니다.

제 9장

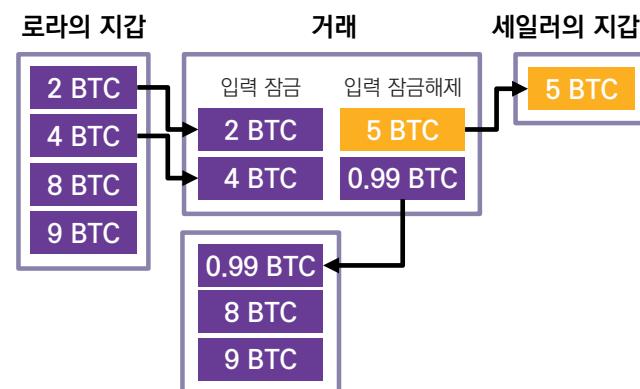


비트코인을 다른 사람에게 보낼 때, 하나 이상의 UTXO를 자금 원천으로 사용하게 됩니다. 필요한 경우 UTXO들이 결합되어 보내는 사람과 받는 사람이 모두 포함된 새로운 출력(UTXO)을 생성합니다. 새롭게 생성된 UTXO들은 각각 보내는 사람과 받는 사람의 자산이 되며, 향후 다시 자금 원천으로 사용될 수 있습니다. 이러한 UTXO의 연속적인 흐름은 비트코인 원장에서 최초 블록부터 시작되는 투명하고 추적 가능한 거래 기록을 형성합니다.

예를 들어, 만약 2 BTC만 보내고 싶지만 5 BTC의 UTXO를 보유하고 있다면, 차액인 3 BTC는 잔돈(change)으로 다시 본인에게 반환됩니다. 이 잔돈은 새로운 UTXO가 되고 향후 다른 거래에서 사용할 수 있습니다.

예시:

- 1 로라는 세일러에게 5개의 비트코인을 보내고 싶어합니다.
- 2 로라는 UTXO에서 총 6개의 비트코인을 결합합니다.
- 3 이 UTXO에서 5개의 비트코인을 세일러에게 전송하고 0.99개의 비트코인을 잔돈으로 자신에게 반환, 0.01개의 비트코인을 전송 수수료로 지불합니다.
- 4 거래가 확인된 후, 비트코인 원장에 기록되며 원장의 사본을 보유한 모든 노드가 업데이트됩니다.



로라가 이미 사용한 UTXO를 다시 사용하여 거래를 시도하면, 노드가 자동으로 거부됩니다. 이는 노드들이 비트코인의 원장과 모든 거래 내역을 보관하고 있기 때문입니다. 따라서, 노드들은 로라의 UTXO 잔액을 쉽게 확인하여 유효하지 않은 거래임을 즉시 알 수 있습니다.

아래의 스크린샷 중 왼쪽은 하나의 입력(input)만 포함된 거래이며 오른쪽은 잔액이 여러 개의 입력으로 되어 있는 실제 사례입니다.

두 거래를 살펴보았을 때, 어떤 차이점을 알 수 있나요? 입력 값과 출력 값이 일치하나요? 거래의 세부 내용을 설명할 수 있나요? 두 거래의 연관성이 있나요? 그리고 어느 거래가 먼저 발생 했을까요?



비트코인 기술 이해

9.3 비트코인 노드와 채굴자에 대한 심층 분석

비트코인 네트워크의 두 가지 중요한 요소인 노드와 채굴자를 자세히 살펴보겠습니다.

1

비트코인 노드(Bitcoin Nodes):

거래의 유효성을 검증하는 역할을 합니다. 비트코인 원장 사본을 유지하고 모든 거래가 유효한지 확인하며, 네트워크의 모든 참여자가 동일한 규칙을 따르도록 보장하는 것입니다.

노드는 전 세계 수많은 사람들이 분산하여 운영하므로 비트코인은 검열 저항성이 있습니다. 또한 비트코인 신뢰성을 유지하며, 중앙 집중화되지 않은 시스템에서 특정 개인이나 단체가 지나친 권력을 가지지 않도록 보장합니다.

2

비트코인 채굴자(Bitcoin Miners):

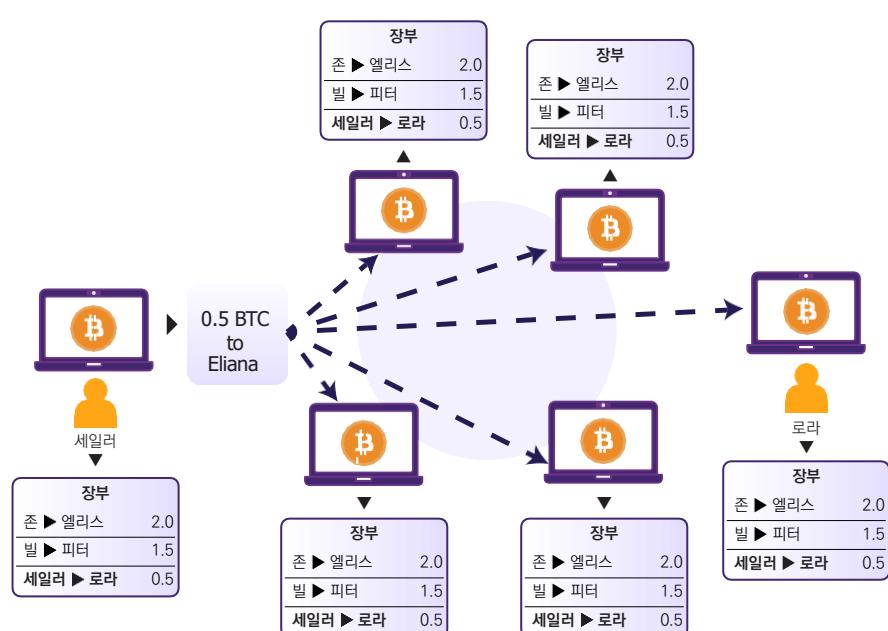
강력한 컴퓨터와 전력을 사용하여 거래를 확인하고 승인하며, 네트워크가 안전하게 유지되도록 합니다. 원장을 악의가 있는 행위자로부터 보호하고 비트코인 시스템이 변조되지 않도록 보장하는 역할을 합니다.

비트코인 노드와 채굴자는 팀처럼 함께 작동하며 탈중앙화되어 강력한 시스템을 유지합니다. 이것은 전 세계 사람들이 신뢰할 수 있는 새로운 금융 시스템을 만들어가는 방식입니다. 이제 그들이 혁신적인 비트코인 시스템에 어떠한 방식으로 기여하는지 더 자세히 알아보겠습니다.

9.3.1 비트코인 노드란 무엇이며, 어떻게 설정하는가?

비트코인 노드라는 개념이 어렵게 느껴질 수 있지만, 비트코인 원장 사본을 실행하는 소프트웨어에 불과합니다. 자신만의 노드를 운영하면 비트코인 네트워크 규칙을 형성하는 과정에서 목소리를 낼 수 있습니다.

예를 들어, 특정 그룹이 비트코인의 총 발행량을 변경하려 한다면 반대 의견을 낼 수 있습니다. 노드를 새로운 시스템으로 변경하지 않는 것만으로도, 기존 네트워크 규칙을 지지하는 투표권을 행사하는 것과 같은 역할을 하게 됩니다.



비트코인 노드를 디지털 교통 경찰에 비유한다면 아래와 같은 역할을 수행합니다.

1

문지기(Gatekeepers of Validation):

비트코인 노드는 타임체인 디지털 사본을 보관하며, 전 세계 노드가 동일한 기록을 유지하고 있습니다. 이것은 모든 비트코인 거래가 기록된 공유 원장과 같습니다.

2

통신 허브(Communication Hub):

노드들은 서로 연결되어 거대한 통신 네트워크를 형성합니다. 특히, 타임체인에 추가되기를 기다리는 거래 정보를 공유하며, 이 정보는 메모리 풀(Mempool)이라는 디지털 대기실에 저장됩니다.

3

품질 검사관(Quality Checker):

타임체인에 추가되는 모든 거래는 철저한 검토를 거칩니다. 노드들은 거래가 유효한지 확인하며, 비트코인 네트워크 규칙을 따르지 않는 거래는 거부합니다.

4

타임체인 정보 제공자(Blockchain Informant):

지갑과 같은 다른 소프트웨어는 노드에게 타임체인 정보를 요청할 수 있습니다. 예를 들어, 비트코인 잔액을 조회할 수 있고 노드는 정보 허브 역할을 수행합니다.

5

새 노드 서포터(New Node Welcomer):

새로운 노드가 네트워크에 합류하려 하면, 기존 노드들은 타임체인 사본을 제공하여 새로운 노드를 돋습니다. 각 거래 유효성을 독립적으로 검증하여 신뢰할 필요 없는(trustless) 시스템 개념을 강화합니다.

체험 활동:

비트코인 노드 영상
시청하기



자신만의 노드를 운영하는 한 가지 방법은 Bitcoin Core 소프트웨어를 다운로드하고, 전체 타임체인을 받을 때까지 기다리는 것입니다. 다운로드가 완료되면, 노드를 계속 실행할 수 있고 약 10분마다 새로운 거래가 포함된 블록이 도착합니다. 이후 노드는 해당 블록의 유효성을 확인하고 자신의 로컬 원장 사본에 추가합니다.

자료:

Bitcoin Core
소프트웨어



노드를 운영하는 것은 주권과 독립성을 제공합니다. 다른 사람에 의존하지 않고, 스스로 비트코인 네트워크를 검증하는 역할을 하게 됩니다. 노드는 비트코인 지갑과 달리 타임체인의 사본을 보유하고 있어 완전한 자기 주권(Self-Sufficiency)이 가능합니다. 즉, 비트코인 보유량이나 네트워크 상태를 다른 사람에게 의존할 필요 없이 지갑과 노드를 직접 통신함으로써, 더 안전하고 신뢰할 수 있는 디지털 환경을 만들 수 있습니다.

비트코인 기술 이해

9.3.2 비트코인 채굴자란 무엇이며, 어떻게 작동하는가?

“

채굴의 목적은 새로운 비트코인을 생성하는 것이 아닙니다. 인센티브 시스템일 뿐입니다.
채굴은 비트코인의 보안을 탈중앙화하는 메커니즘입니다.

안드레아스 M. 안토노풀로스

”

채굴자들은 다음 블록을 타임체인에 추가하기 위한 경쟁을 하고 있습니다. 이들이 원하는 것은 유효한 블록 해시(valid block hash)이며, 이 해시는 수십억 개의 다른 해시 값들 사이에 숨겨져 있어 네트워크가 할당한 특정 키만이 해독할 수 있습니다.

거대한 건초 더미 속에 수백만 개의 열쇠(각각의 블록 해시)가 흩어져 있다고 상상해보세요. 네트워크는 이 중 특정한 하나의 열쇠만이 보상을 받을 수 있도록 선택됩니다. 채굴자들은 건초 더미를 뒤지며 열쇠를 하나씩 테스트하지만, 오직 하나의 채굴자만 정확한 키를 찾아낼 수 있습니다.

채굴자가 올바른 블록 해시를 찾으면, 새로운 거래들이 포함된 블록과 함께 네트워크에 공유합니다. 다른 채굴자들은 해시를 검증하여 정확한 해답인지 확인하고 타임체인에 추가하며, 안전하고 공개적인 원장이 형성됩니다.

채굴자들은 노력의 보상을 두 가지 방식으로 받습니다.

1

블록 보상

2

전송 수수료

블록 보상(Block Rewards)은 새로운 비트코인이 발행되어 유통되는 방식으로, 각 블록이 타임체인에 추가될 때마다 새롭게 생성됩니다. 전송 수수료(Transaction Fees)는 채굴자의 우선순위를 받을 수 있도록 지불하는 소액의 비트코인입니다. 채굴자들은 채굴하는 블록에 어떤 거래를 포함할지 선택할 수 있지만, 보통 전송 수수료가 높은 것을 먼저 선택합니다.

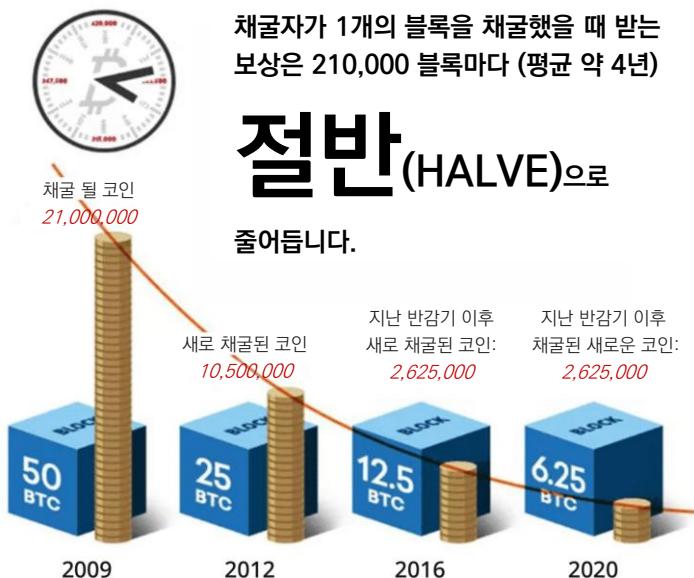
비트코인 반감기 (Bitcoin Halvings)

비트코인 반감기는 비트코인 희소성과 가치를 유지하는 중요한 메커니즘입니다. 비트코인의 총 발행량은 2,100만 개로 고정되어 있지만, 모든 비트코인이 출시된 날부터 즉시 유통된 것은 아닙니다. 단계별 방식으로 공급되도록 설계되었습니다.

사토시 나카모토(Satoshi Nakamoto)는 중앙 기관 없이 새로운 비트코인을 분배할 수 있도록 블록 보상 시스템을 정교하게 설계했습니다. 비트코인 초창기에는 채굴자들이 블록을 채굴할 때마다 50 BTC라는 높은 보상을 받았습니다. 이 보상은 채굴자들이 기계와 전기 비용에 투자하여 채굴을 지속할 동기가 되었습니다.

채굴자가 1개의 블록을 채굴했을 때 받는 보상은 210,000 블록마다 (평균 약 4년)

절반(HALVE)으로 줄어듭니다.



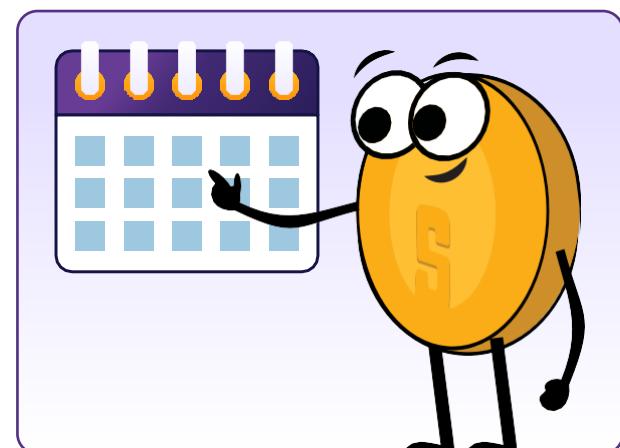
네트워크를 안정적으로 유지하고 새로운 비트코인 공급을 조절하기 위해, 블록 보상은 210,000블록마다 절반으로 줄어듭니다. 이를 “반감기(the halving)”라고 부르며, 유통되는 비트코인의 개수를 감소시키고 채굴자들이 네트워크를 보호하며 탈중앙화를 유지할 동기를 부여합니다. 역사적으로 반감기는 새로운 비트코인 공급 감소로 인해 시장에서 가격 상승을 초래했습니다.

유통 발행량(Circulating Supply)은 전체 통화량을 의미합니다. 비트코인의 총 유통 발행량은 현재까지 채굴되어 유통 중인 비트코인의 개수를 나타내며, 영구적으로 분실된 코인은 제외됩니다.



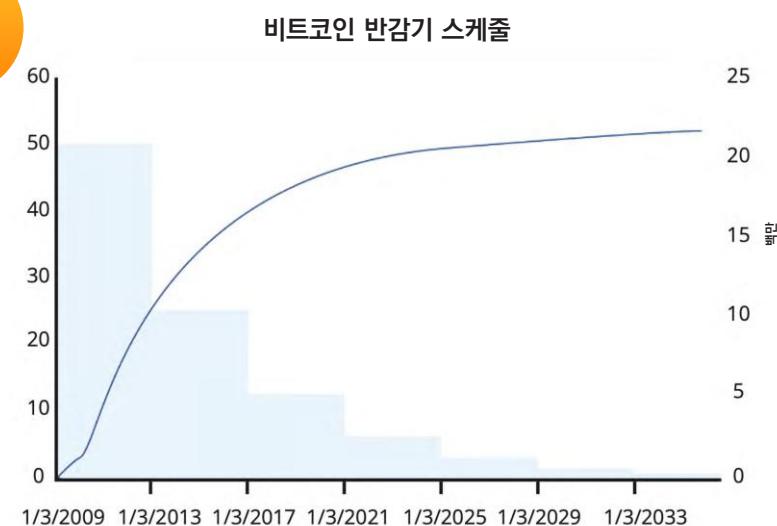
각 반감기마다 채굴자들이 받는 비트코인 보상이 줄어들며, 새로운 코인의 발행 속도가 감소합니다. 비트코인의 채굴 난이도는 블록 생성 시간을 약 10분으로 유지시키며, 새로운 블록이 일정한 시간으로 타임체인에 추가될 수 있습니다. 채굴 보상이 감소한다고 해서 채굴자들의 수익이 반드시 줄어드는 것은 아닙니다. 채굴자들은 거래를 검증하고 타임체인에 추가하는 과정에서 전송 수수료를 받아 채굴 보상 감소분을 상쇄할 수 있습니다.

반감기는 비트코인 프로토콜에 미리 프로그래밍되어 있어, 비트코인 공급 일정이 예측 가능하고 투명하게 유지됩니다.



비트코인의 공급 일정(Bitcoin Supply Schedule)은 새로운 비트코인이 유통될 계획을 미리 정해둔 공개된 프로토콜로, 시간이 지남에 따라 비트코인 희소성을 유지하도록 설계되었습니다.

다음 표는 비트코인의 향후 반감기 세부 사항을 정리한 것입니다. 여기에는 다음 반감기 예상 날짜, 반감기가 발생할 블록 높이, 해당 반감기에 받는 블록 보상(채굴된 블록당 지급되는 비트코인), 전체 발행량 중 채굴될 비율이 포함되어 있습니다.



스케줄	예상 날짜	블록 높이	블록 보상	채굴된 비트코인(%)
네 번째 반감기	2024	840,000	3.125	96.875 %
다섯 번째 반감기	2028	1,050,000	1.5625	98.4375 %
여섯 번째 반감기	2032	1,260,000	0.78125	99.21875 %

비트코인 기술 이해

더 많은 비트코인이 채굴될수록 유통
발행량과 전체 발행량 중 채굴된 비율은 계
속 증가하며, 궁극적으로 총 2,100만 개의
비트코인이 모두 채굴될 때까지 지속됩니다.
반감기로 인해 새로운 비트코인의 공급이
감소하면, 비트코인 가격 상승 가능성이
높아집니다. 결국 초기 비트코인 사용자들
에게 이익이되며, 채굴자들이 계속해서 네
트워크를 보호하고, 연산 능력과 자원을 제
공할 동기를 부여합니다.

비트코인: 총 2,100만 개 발행량 중 채굴된 비율 (%)



비트코인에서 유효한 블록 해시란 무엇인가?

비트코인에서 유효한 블록 해시는 채굴자들이 찾고자 하는 특별한 코드와 같습니다. 이것은 각 블록을 추적하는 고유한 숫자로
타임체인에서 거래 정보를 저장하는 모든 블록을 식별하는 역할을 합니다. 비트코인의 블록들은 첫 번째 블록(제네시스 블록)
부터 최신 블록까지 연결된 체인 형태를 이루며, 모든 거래 내역이 기록된 공개 원장 역할을 합니다. 유효한 블록 해시는 각
블록이 이전 블록과 연결되도록 하며, 누구나 거래의 진위 여부를 쉽게 확인할 수 있도록 만듭니다. 각 블록에 해당하는 지문
(fingerprint)과 같은 역할을 하며, 해시를 통해 블록 데이터가 변경되지 않았음을 보장합니다.



블록들은 특정한 관계로 연결됩니다. 각 블록에는 이전 블록
데이터에 대한 해시가 포함되어야 합니다. 이 해시는 이전 블
록의 데이터를 해시한 값입니다. 해시 함수(hash function)
는 임의의 블록 정보를 압축하여 고정된 크기 값으로 변환
하며, 메시지의 고유한 해시를 생성합니다.



비트코인의 창시자인 사토시 나카모토는 최초의 블록을 채굴했으며, 블록 보상으로 50 비트코인이 포함
되어 있었습니다. 하지만 사토시 나카모토는 최초 블록을 혼자만 채굴했기에 공정하지 못하다며, 자신을
포함해 아무도 사용하지 못하게끔 코드로 프로그래밍했습니다.





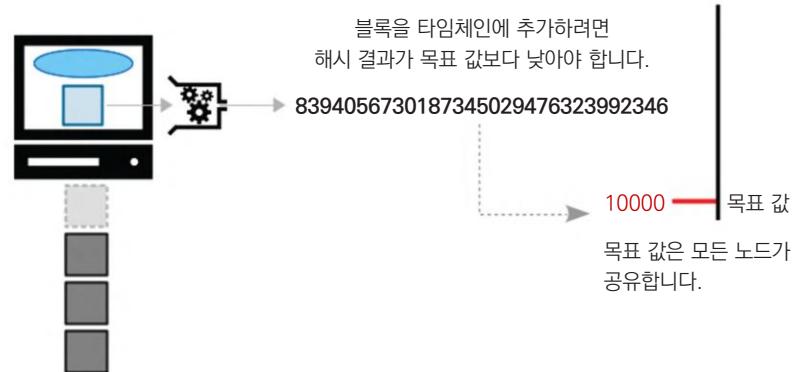
제 9장

블록 채굴 경쟁

채굴자들은 네트워크가 설정한 목표 값에 맞는 블록 해시(block hash)를 찾기 위해 경쟁합니다. 가장 먼저 올바른 블록 해시를 찾아낸 채굴자는 해당 블록을 타임체인에 추가할 기회를 얻게 되고 해시 ID를 부여할 수 있습니다. 이 과정은 블록 신뢰성과 정당성을 검증하는 역할을 합니다.

채굴은 결승선에 제일 먼저 도착해야 하는 경주에 비유할 수 있습니다.

블록 해시를 찾는 난이도는 일정 주기마다 조정되며, 채굴자(해시)가 늘어나거나 줄어들어도 블록은 약 10분 간격으로 채굴되도록 유지됩니다. 이 메커니즘을 “난이도 조정(Difficulty Adjustment)”이라고 합니다



비트코인 네트워크에서 설정한 목표 숫자가 1,000이라고 가정해 봅시다. 채굴자들은 연산 능력과 전기를 사용하여 1,000보다 작은 블록 해시 값을 찾기 위해 계산을 수행해야 합니다. 가장 먼저 1,000보다 작은 블록 해시 값을 찾은 채굴자가 새로운 블록을 타임체인에 추가할 수 있는 권한을 얻으며, 보상으로 비트코인을 받게 됩니다.

비트코인 채굴 난이도(Difficulty Level)는 네트워크가 설정한 목표 값보다 작은 블록 해시 값을 찾는 것의 난이도를 나타내는 척도입니다. 이 난이도는 2016 블록마다(약 2주 간격으로) 조정되며, 블록이 일정한 속도로 타임체인에 추가되도록 보장합니다. 난이도는 숫자로 표현되며, 난이도가 높을수록 블록 해시 값을 찾기가 더욱 어려워집니다.

예를 들어, 두 개의 서로 다른 해시를 비교해 보겠습니다.

해시 1: 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK
난이도 레벨: 1

해시 2: 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK
난이도 레벨: 2

위의 예시에서 해시 2는 해시 1보다 난이도가 더 높습니다. 그 이유는 해시 값 앞부분에 0이 더 많이 포함되어 있기 때문입니다. 즉, 채굴자들이 해시 2를 찾는 것은 해시 1을 찾는 것보다 훨씬 더 어렵고 많은 연산 작업이 필요합니다.

채굴자가 블록 해시 값을 찾으면 블록을 타임체인에 추가하는 데 필요한 작업을 수행했음을 증명하는 것입니다. 그 대가로 비트코인 보상과 전송 수수료를 받게 됩니다. 이 과정은 비트코인 네트워크가 거래를 검증하고 새로운 블록을 블록체인에 추가하는 데 사용하는 합의 메커니즘이며, 작업 증명(Proof-of-Work, PoW)라고 부릅니다.

비트코인 기술 이해

작업 증명(PoW)은 악의가 있는 사람이 비트코인 장악을 어렵게 만들어 네트워크를 안전하게 보호합니다. 채굴자 역할을 요약하면 다음과 같습니다:

1

거래를 블록으로 묶기(Bundling Transactions into Blocks):

노드들은 메모리풀(Mempool)에 있는 신규 거래를 검증하며, 채굴자들은 일부를 선택하여 자신의 후보블록(candidate block)에 포함합니다.

2

작업 증명(Proof-of-Work):

채굴자들은 유효한 블록 해시(valid block hash)를 찾기 위해 경쟁합니다.

3

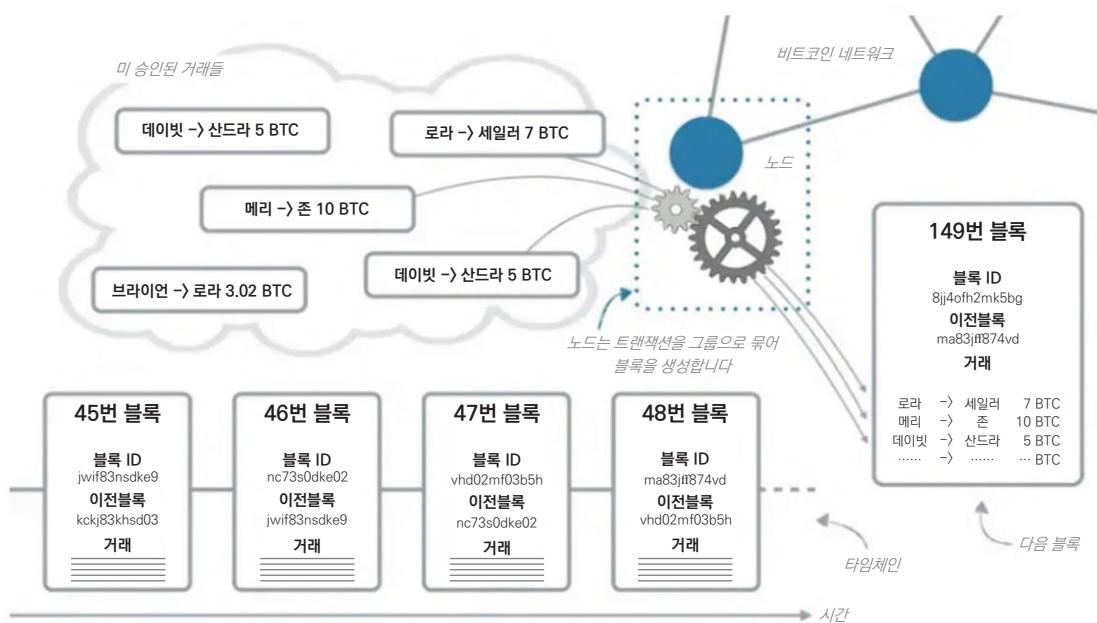
유효한 블록을 네트워크에 전파(Broadcast Valid Blocks):

유효한 블록 해시를 찾은 후, 새로운 블록을 네트워크에 전파(propagate)합니다.

4

보상 획득(Earn Rewards):

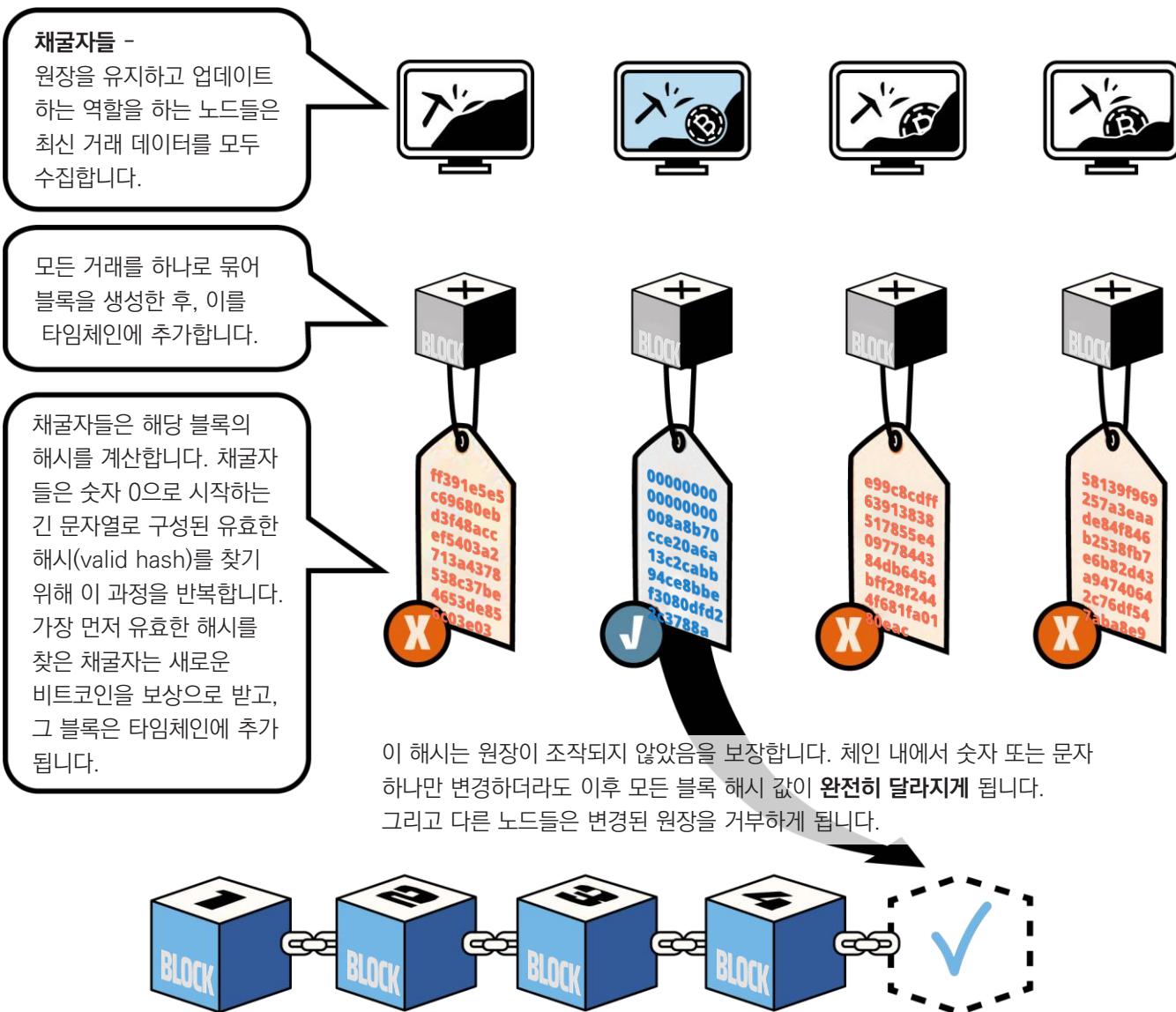
블록을 타임체인에 성공적으로 추가한 채굴자는 새롭게 생성된 비트코인과 전송 수수료를 보상으로 받습니다.



여러 채굴자가 새로운 블록을 생성하는 작업을 동시에 할 수 있습니다. 네트워크가 설정한 목표 값에 맞는 블록 해시를 가장 먼저 발견한 채굴자는 이를 네트워크에 발표하며, 다른 채굴자들은 해당 채굴자의 후보블록(candidate block)에 포함된 거래들을 검토하여 유효성을 확인합니다. 만약 거래가 유효하다고 검증되면 해당 블록이 타임체인에 추가되고 다른 채굴자들이 생성한 블록은 추가되지 않고 폐기됩니다. 이 과정은 네트워크 합의를 유지하고, 이중 지불(double-spending)을 방지합니다.

후보 블록(candidate block)이란 아직 타임체인에 추가되지 않은 거래들의 집합을 의미합니다.





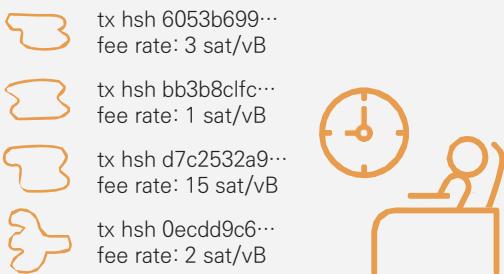
9.4 메모리 풀(Mempool)이란 무엇인가?

메풀(Mempool) 또는 메모리 풀(memory pool)은 비트코인 네트워크에서 거래가 타임체인에 추가되기 전에 대기하는 공간과 같습니다. 개인키 서명을 통한 거래가 브로드캐스트 되면 메모리 풀에 전송된 후 검증과 채굴자의 선택을 통해 타임체인에 추가됩니다.

레스토랑 대기줄에 비유할 수 있습니다. 음식을 먹기 위해 대기 명단에 이름을 올리고 번호를 호출할 때까지 기다려야 합니다. 직원은 테이블이 비면 번호를 불러 자리로 안내합니다. 비트코인도 거래가 생성되면 메모리 풀에 추가됩니다. 그 후, 채굴자가 해당 거래를 블록에 포함하면, 거래가 확인되어 타임체인에 추가됩니다.

비트코인 기술 이해

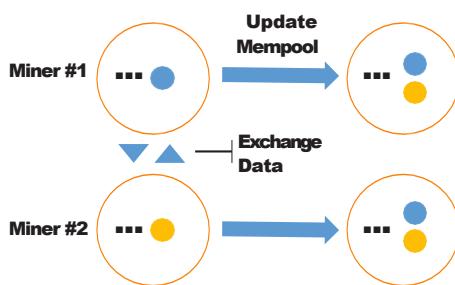
메모리 풀은 거래가 블록에 포함되어 확인될 때까지 대기하는 공간입니다.



노드가 피어(peer)로부터 처음 거래들을 받으면, 해당 거래가 정상적인지 검증해야 합니다. 아무도 조작된 거래를 원하지 않기 때문입니다.



메모리 풀 동기화(mempool synchronization)는 노드들이 검증된 거래 목록이 포함된 메시지를 전송하여, 다른 노드들과 거래를 공유하는 것입니다.



거래가 검증되어 메모리 풀에 추가되는 원리는 무엇인가?

새로운 거래가 비트코인 네트워크에 전파되면, 노드들은 해당 거래의 유효성과 자금의 사용 여부를 검증합니다. 검증이 완료되면 해당 거래를 노드 자신의 메모리 풀(Mempool)에 추가합니다. 그 후, 거래를 다른 노드들과 공유하여 이중 검증(Double-checking)을 진행합니다. 마지막으로, 대부분의 노드들이 해당 거래가 유효하다고 동의하면 채굴자들이 거래를 선택하여 블록에 포함할 수 있도록 공개됩니다. 그러나 거래가 72시간이 지나도 확인되지 않을 수 있는 몇 가지 이유가 있습니다.

메모리 풀의 주 목적:

1

미확인 거래를 중계.



2

채굴자들에게 채굴할 거래를 제공.



메모리 풀에 거래를 승인하는 과정에서는 다음과 같은 사항을 확인해야 합니다:

- 이미 해당 거래를 보유하고 있는가?
- 메모리 풀 내에서 다른 거래와 중복하지 않는가?
- 비트코인을 보내는 수량보다 많은가?
- UTXO 사용 가능한 개인키인가?
- 수수료가 충분한가?

1 낮은 전송 수수료(Low Transaction Fees):

채굴자들이 더 높은 수수료의 거래를 우선적으로 선택하기 때문에 전송 수수료가 낮다면 우선순위가 밀릴 수 있습니다.

2 네트워크 혼잡(Network Congestion):

네트워크가 혼잡할 경우, 전송 수수료를 많이 지불 했더라도 확인(검증)에 지연이 발생할 수 있습니다.

3 이중 지불 시도(Double Spend Attempt):

악의가 있는 사용자가 이중 지불(double spending)을 시도하면, 해당 거래는 네트워크가 거부할 수 있습니다.

4 잘못되거나 불완전한 데이터(Incorrect or Incomplete Data):

거래에 잘못된 정보나 불완전한 데이터가 포함되어 있을 경우, 해당 거래는 네트워크에서 거부될 수 있습니다.

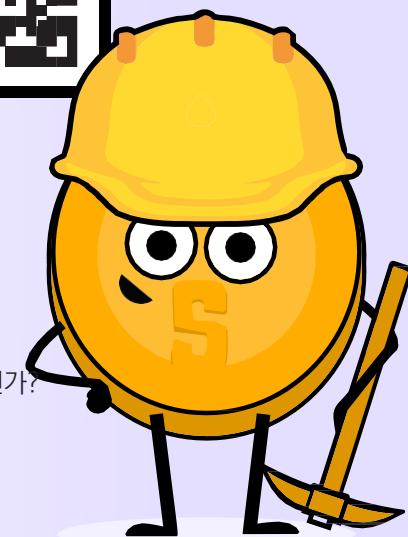
5 잘못된 형식의 거래(Malformed Transaction):

거래 형식이 올바르지 않을 경우, 네트워크에서 해당 거래를 거부할 수 있습니다.

거래가 지연되지 않도록 하려면 높은 수수료를 설정하는 것이 좋습니다. 또한 거래를 전송하기 전에 모든 데이터가 올바른지 꼼꼼히 확인하는 것도 중요합니다.

체험 활동: 메모리풀**1 QR code를 스캔합니다:****2 페이지에 표시된 다양한 요소를 검토합니다.**
여기에는 죄신 블록, 확인된 거래, 거래 수, 메모리 사용량, 그리고 전체 블록의 가치가 포함됩니다. 다음 질문에 답하세요:

- 💡 해당 블록에 포함된 총 거래 수는 몇 건인가?
- 💡 해당 블록에서 총 거래된 비트코인 가치는 얼마인가?
- 💡 블록의 크기는 몇 메가바이트(MB)인가?
- 💡 블록의 논스(Nonce)는 몇 개의 0(zeros)로 시작하는가?
- 💡 채굴자는 총 몇 비트코인을 보상으로 받았는가?
- 💡 채굴자가 거래를 네트워크에 추가하면서 받은 총 수수료 가치는 얼마인가?
- 💡 블록 내 가장 높은 가치의 거래 중 하나를 선택하세요.
- 💡 해당 거래에서 비트코인은 몇 개의 주소로 분배되었는가?



비트코인 기술 이해

9.5 비트코인 거래의 시작부터 완료까지의 과정

1

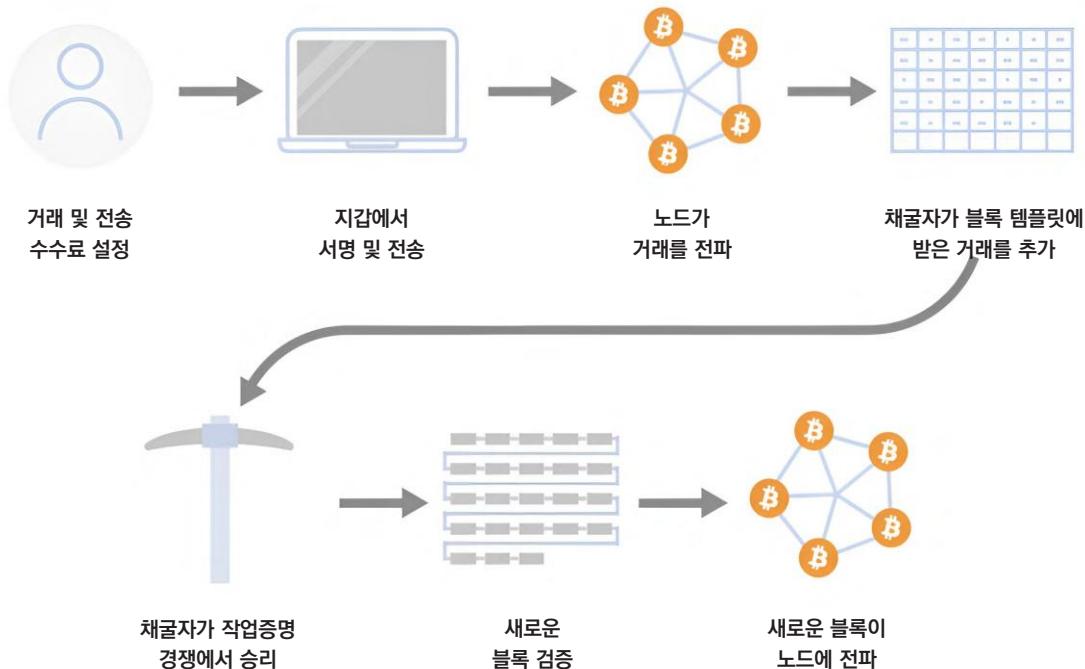
아담백은 세일러에게 비트코인을 보내고 싶어 합니다. 그리고 아담백은 UTXO 중 하나를 선택하여 거래를 생성한 뒤, 보낼 비트코인의 개수, 세일러의 비트코인 주소, 그리고 전송 수수료를 포함한 모든 필수 정보를 추가합니다.

2

모든 입력 사항이 올바른지 최종 확인 후 개인키를 사용하여 거래에 서명합니다.

3

해당 거래를 비트코인 네트워크에 전파(broadcast)합니다.



출처: Stevenot, Ted, “비트코인 노드란 무엇이며 작동하는 원리는 무엇인가?”
Unchained Capital, 2023년 1월 17일,

4

네트워크의 노드들은 해당 거래를 받은 후, 합의 규칙(Consensus Rules)에 따라 거래의 유효성을 검증합니다.
(예: 서명이 유효한지, 거래를 수행할 충분한 잔고가 있는지 확인).

5

거래가 유효한 것으로 확인되면, 네트워크의 다른 노드들에게 전파(Propagate)하며, 메모리 폴에 추가합니다.

6

충분히 높은 전송 수수료를 설정했기에, 대부분의 채굴자들은 그 거래를 블록에 포함하려고 합니다.



제 9장

7

채굴자들은 유효한 블록 해시(valid block hash)를 찾기 위해 경쟁하며, 가장 먼저 해시를 찾은 채굴자는 블록을 네트워크에 전파(broadcast)합니다.

8

네트워크의 노드들은 새로 채굴된 블록을 받은 후, 블록 내 모든 거래를 검증하고 작업 증명(Proof-of-Work) 요구사항의 충족 등 해당 블록의 유효성을 검증합니다.

9

다수의 노드들이 해당 블록이 유효하다고 동의하면 블록은 타임체인에 추가됩니다. 그 순간 세일러는 자신의 주소에서 비트코인을 확인할 수 있습니다.

10

이후 추가되는 블록들이 타임체인에 계속 연결되면서, 거래 확인 횟수(confirmations)가 증가합니다. 거래 확인 횟수가 증가할 수록, 거래를 되돌릴 수 없다는 것(irreversible)임을 더욱 확신하게 됩니다.

받는 사람은 개인키로 거래에 서명하고, 노드들은 거래의 UTXO를 검증하며, 채굴자들은 검증된 거래를 타임체인에 추가합니다. 이후, 받는 사람은 개인키를 사용하여 비트코인을 통제 할 수 있습니다. 블록이 채굴되면, 해당 블록에 포함된 모든 거래는 확인(confirmed)된 것으로 간주되며, 거래에서 입력으로 사용된 UTXO는 이미 사용된 것으로 처리되므로 다시 사용할 수 없습니다.



이 장에서는 비트코인이 작동하는 기본 개념을 배웠습니다. 우리는 화폐의 기초부터 비트코인 기술까지, 핵심적인 내용을 다루었습니다. 다음 장에서는 모든 내용을 연결해보며, “왜 비트코인인가?”라는 중요한 질문을 깊이 탐구할 것입니다.

제 10장

왜 비트코인인가?

10.0 서론

체험 활동: 비트코인은 미래는 어떤 모습일까?

10.1 중앙은행 디지털 화폐(CBDC)란 무엇이며, 누가 통제하는가?

10.2 비트코인 철학

체험 활동: 수업 토론 - 여러분은 돈을 통제할 권리가 있는가?

10.3 비트코인 이점

10.4 보장된 미래

체험 활동: 수업 토론 - 여러분의 관점은 어떻게 변했는가?

추가 자료

핵심 개념

용어집

왜 비트코인인가?

10.0 서론

“

비트코인은 단순한 화폐가 아니다.
비트코인은 혁명이며, 금융 주권을 사람들에게 되돌려주고,
자유와 평화를 갈망하는 세상에 희망을 제시하는 변화의 바람이다.

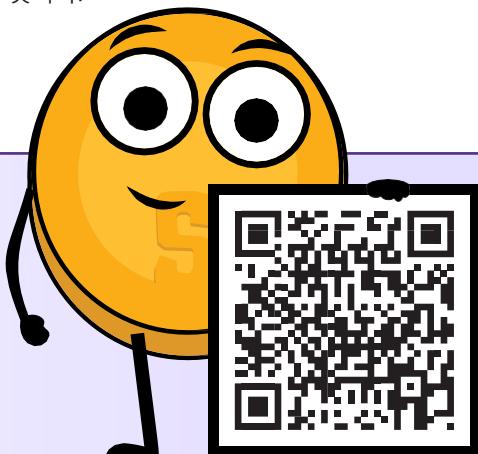
My First Bitcoin

”

이 마지막 장에서는 지금까지 배운 내용을 정리하고, 몇 가지 질문을 던지며 비트코인이 펼칠 미래에 대해 탐구해 보려 한다.

비트코인은 단순한 기술이 아니다. 새로운 형태의 화폐를 구동하는 네트워크이며, 발행량은 아무도 변경할 수 없다. 인류는 역사상 중앙에서 통제되지 않고 발행량이 고정된 화폐를 가져본 적이 없었다. 만약 비트코인이 널리 채택된다면, 전 세계 사람들의 삶을 변화시키는 도구가 될 것이며, 평화로운 혁명을 통해 자유와 공정함을 추구하는 길을 열어줄 것이다. 비트코인은 모두가 공유하는 글로벌 통화 시스템을 창출함으로써, 인류에게 새로운 기회를 제공한다.

비트코인은 중앙 집중화된 금융 시스템을 넘어서는 글로벌 네트워크이다. 비트코인은 금융 자유를 확대시키고, 소수가 쥐고 있는 금융 주권을 모든 사람에게 분산시키는 힘을 가진다. 이를 통해 겸열 저항성을 제공하며, 개인이 부를 보호하고 구매력을 유지할 수 있도록 힘을 실어준다. 이는 특히 오늘날 불확실한 경제 상황에서 더욱 중요하다. 기존 금융 시스템이 전례 없는 위기에 직면한 이 시대에 비트코인은 새로운 희망과 변화를 가져오는 도구가 될 것이다.



체험 활동: 비트코인의 미래는 어떤 모습일까?

비트코인에는 더 나은 변화 가능성이 무궁무진합니다.
더 자세히 알아보기 위해서 이 영상을 시청해 보세요.

다음으로, 중앙은행 디지털 화폐(CBDC, Central Bank Digital Currency)라는 또 다른 형태의 디지털 화폐를 살펴보고, 비트코인과 다른 점은 무엇인지 평가해 보겠습니다.

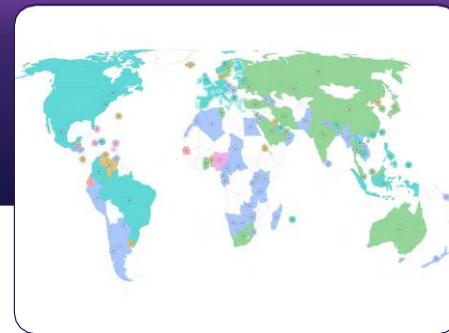
10.1 중앙은행 디지털 화폐란 무엇이며, 누가 통제하는가?

중앙은행 디지털 화폐(CBDC, Central Bank Digital Currencies)는 기존 명목화폐(fiat money) 디지털 버전입니다.

중앙은행 디지털 화폐 이하 CBDC는 기존 명목화폐와 마찬가지로 정부와 같은 중앙 기관이 발행량을 조절할 수 있으며, 사람들의 구매력이 감소할 수 있습니다. 그러나 CBDC는 단순한 디지털 화폐를 넘어, 정부가 개인이 보유한 돈을 보다 강력하게 통제할 수 있는 도구를 제공합니다.

여러분 국가가 중앙은행 디지털 화폐를 도입하고 있는지
확인하려면, 인권재단(HRF) CBDC 추적 사이트를 방문하세요.

<https://cbdctracker.hrf.org/home>
<https://cbdctracker.org/>



그렇다면, CBDC는 기존 명목화폐와 무엇이 다를까?

CBDC는 단순히 디지털 형태라는 점 외에도 기존 명목화폐와 중요한 차이점이 있습니다. 그것은 CBDC가 모든 거래를 정부가 디지털 방식으로 감시하고 통제할 수 있도록 한다는 것입니다. 즉, 정부가 특정 거래를 차단하거나, 심지어 계좌 전체를 동결할 수도 있습니다. 단순히 정부가 여러분을 좋아하지 않거나, 돈을 사용하는 방식이나 사용처가 마음에 들지 않기 때문일 수도 있습니다.

예를 들어, 가족이 다른 국가에 거주하고 있어 송금을 하려 하지만, 여러분의 정부가 해당 국가의 지도자를 좋아하지 않는다는 이유로 거래를 거부한다면? 여러분이 SNS에서 정치 성향을 표현했다는 이유만으로, 가게에서 물건을 사고 싶어도 결제가 차단된다면? 이것이 CBDC가 기존 명목화폐와 완전히 다른 점입니다.

CBDC는 정부가 돈의 사용 방식을 무제한으로 통제할 수 있으며, 개인이 돈을 사용할 권리를 제한합니다. 일부에서는 CBDC가 강력한 정부 무기 중 하나로 전 세계에 독재 정책을 밀어붙일 수 있는 도구가 될 것이라고 주장합니다. 즉, 별도의 감시 요원 없이 중앙에서 강력한 통제를 실행할 수 있는 수단이 된다는 것입니다.

CBDC와 비트코인은 둘 다 디지털화폐이지만, 그 외에는 완전히 다른 철학과 원칙을 기반으로 설계된 화폐입니다. 결국 CBDC와 비트코인은 인류에게 매우 다른 영향을 미칠 것이며, 각각 상반된 미래를 만들어갈 가능성이 큽니다.



왜 비트코인인가?

10.2 비트코인 철학

6장과 9장에서 노드를 운영하는 개인들이 비트코인 규칙을 보호하는 역할을 한다는 것을 배웠습니다. 사상 최초로 우리 같은 평범한 사람들이 직접 참여하여 화폐 시스템을 보호하는 역할을 할 수 있다는 점은 매우 중요한 의미를 가집니다. 비트코인은 총 발행량이 고정되어 있으며, 어떤 주체도 마음대로 변경할 수 없습니다. 즉, 모든 사람들이 화폐 신뢰성을 보장 받을 수 있습니다.

비트코인은 자율성(Empowerment), 자유(Freedom), 금융 독립(Financial Independence), 비판적 사고(Critical Thinking), 그리고 자신이 속한 시스템 규칙을 결정할 수 있어야 한다는 개념을 기반으로 합니다. 기존 명목화폐 시스템은 강력한 중앙 기관이 통제하지만, 비트코인은 어떠한 주체도 완전한 통제권을 가질 수 없는 네트워크에서 운영됩니다. 즉, CBDC와 같은 기존 화폐 시스템과 달리 비트코인에서는 어떤 정부나 기관도 여러분 돈을 압류하거나 사용하는 것을 막을 수 없습니다.

기존 명목화폐 시스템에서는 많은 부를 가진 사람이 더 많은 권력과 영향력을 가지게 됩니다. 하지만 비트코인은 사람들에게 금융 주권을 돌려주며, 가진 부와 상관없이 시스템을 유지하는 데 중요한 역할을 합니다. 비트코인은 합의된 규칙을 바탕으로 운영되며, 인류 전체가 함께 운영해 나가는 힘을 가집니다. 즉, 소수의 사람들이 모든 결정을 내리는 것이 아니라 우리 모두가 함께 협력하여 비트코인 방향을 결정하는 것입니다.

명목화폐 시스템에서는 권력을 가진 자들이 규칙을 정합니다. 하지만 비트코인 네트워크에서는 개인들 공동의 힘이 시스템을 유지합니다. 어떠한 개인도 비트코인 생태계를 마음대로 조정할 수 없습니다. 이것이 기존 금융 시스템의 권력 구조를 완전히 뒤집는 방식입니다. 비트코인의 진정한 목표는 투명하며, 공정한 금융 시스템을 구축하는 것입니다.

이를 통해 모든 사람이 글로벌 금융 시스템에 접근할 수 있는 세상을 만드는 것이 핵심입니다.

체험 활동: 수업 토론 – 여러분은 돈을 통제할 권리가 있는가?

- 1** 돈은 인간에게 필수인가? 그리고 인간의 기본권인가? 그 이유는 무엇인가?
- 2** 만약 우리가 원하는 방식으로 돈을 사용할 수 없고, 원하는 사람에게 보낼 수도 없으며, 새로운 나라로 이동할 때 돈을 자유롭게 가져갈 수도 없다면, 그것이 정말 돈이라고 할 수 있을까? 그 이유는 무엇인가?
- 3** 물물교환은 왜 더 이상 하지 않게 되었는가? 쌍방 요구 일치(double coincidence of wants)는 무엇이며, 어떤 문제가 있는가?
- 4** 역사적으로 여러분에게 가장 큰 영향을 준 사건은 무엇인가? 닉슨 쇼크(Nixon Shock)를 이해하는 것이 오늘날 우리에게 왜 중요한가?
- 5** 발행량이 고정된 화폐와 기존 명목화폐는 다른점은 무엇이고, 어떤 영향을 미치는가?
- 6** 비트코인은 누가 언제 어떤 목적으로 만들어졌으며, 탈중앙화 시스템의 개념은 무엇인가?



제 10장

- 7 셀프커스터디 지갑과 수탁 지갑의 차이점은 무엇인가? 여러분이 가장 좋아하는 지갑은 무엇이었는가?
- 8 라이트닝 네트워크(Lightning Network)에 대해 이해하며, 어떤 종류의 거래에 사용할 수 있을까?
- 9 자신만의 노드를 운영하는 것이 비트코인 네트워크를 어떤 방식으로 기여하는가?
- 10 돈을 직접 통제할 수 있다는 것은 일상생활과 미래 계획에 어떤 영향을 주는가?
- 11 금융 주권은 지역 사회나 국가에 어떠한 긍정적인 기여를 하는가?

10.3 비트코인 이점

하이퍼비트코이네이션(Hyperbitcoinization)은 비트코인이 전 세계의 화폐 시스템이 되는 미래를 의미합니다. 모든 사람이 어디에서나 비트코인을 사용하는 세상을 뜻하며, 커피를 사는 것부터 세금을 내고 부동산을 구입하는 것까지 포함됩니다.

개인, 기업, 국가가 비트코인에 점점 더 많은 관심을 보이고 있으며, 비트코인을 많은 곳에서 받아들일 때 경제와 사회에 미칠 앞으로 나타날 영향을 강조합니다. 다음은 하이퍼비트코이네이션이 실현될 경우 기대할 수 있는 몇 가지 이점입니다:

1 주권이 보장된 미래:

주권이 보장된 미래란 전 세계 개인들이 디지털 정체성과 자산을 완전히 통제할 수 있는 세상을 의미합니다. 이는 누구나 금융을 편하게 쓸 수 있도록 넓히고, 자유, 프라이버시, 보안 강화로 이어질 수 있으며, 결국 인간이 번영하고 풍요롭게 행복을 높이는 데 도움이 될 수 있습니다.

2 신뢰할 수 있는 가치 저장 수단:

비트코인은 디지털 희소성을 갖추고 있어 신뢰할 수 있는 가치 저장 수단이 됩니다. 더 많은 사람에게 미래를 위한 저축 수단으로 활용하도록 장려할 수 있습니다.

3 통화 정책의 변화:

비트코인이 많이 수용될 경우, 정부가 기존 통화정책을 통해 화폐 발행 능력을 감소 시킬 수 있습니다. 비트코인은 사람들 구매력을 높이고, 오랜 시간 동안 가치 있는 활동에 집중하도록 유도할 가능성이 있습니다.

4 강화된 투명성과 추적 가능성:

타임체인에 기록된 모든 거래는 변조할 수 없고 끝없이 보존되므로, 다양한 산업과 분야에서 감추는 것 없이 책임감을 높일 수 있습니다. 현재 권력을 보유한 기관들은 세계 곳곳에 수조 달러를 이동시키면서도 자금이 어디로 가고 사용되는지 명확히 공개하지 않는 경우가 많습니다. 비트코인은 투명하고 검증 가능한 금융 거래 기록을 제공함으로써, 자본 흐름을 보다 책임감 있고 대중에게 접근 가능하게 만들 수 있습니다.

왜 비트코인인가?

송금 시장 혁신:

5

송금 시장은 사람 간 국가 간 자금을 이전하는 것을 포함합니다. 송금 비용이 점차 감소하고 있음에도 여전히 해외 송금은 국내 은행 이체에 비해 비싸며, 소액 송금은 더욱 그렇습니다. 라이트닝 네트워크는 빠르고 저렴하며 송금 시장에 적합한 솔루션이 될 수 있습니다. 이를 통해 송금 수수료뿐만 아니라, 긴 정산 시간과 영업시간 제한 등 기존 송금 문제를 해결할 수 있습니다.

풍부한 에너지:

6

풍부하고 저렴한 에너지가 있다면 사회는 번영할 수 있으며, 다양한 산업과 지역사회가 가정, 기업, 그리고 새로운 기술이 증가하는 전력 수요를 충족할 수 있게 됩니다. 비트코인 채굴은 태양광, 풍력, 수력과 같은 지속 가능한 에너지원에서 발생하는 잉여 에너지를 활용하도록 채굴자들에게 인센티브를 제공합니다. 채굴자들은 이 잉여 에너지를 사용하여 비트코인을 채굴하고 네트워크를 보호하며, 필요할 때 에너지 그리드(전력망)에 남는 에너지를 다시 공급함으로써 사회에 기여할 수 있습니다.

10.4 보장된 미래

비트코인은 돈입니다.

돈은 사람들이 상품과 서비스를 교환하며 사회활동을 하는 중요한 소통 수단입니다. 이 과정에서 배운 바와 같이 돈을 중앙 기관이 통제하면 조작될 위험이 있습니다.

인류는 오랜 기간 되풀이해서 화폐를 조작해 왔고, 결국 개인, 가족, 기업, 정부 그리고 세계 곳곳에 바람직하지 않은 영향을 미쳤습니다.

중앙 기관이 돈을 통제하는 구조에서 벗어나, 누구도 변경할 수 없는 고정된 발행량을 가진 돈을 사용한다면, 완전히 새로운 세상을 만들 수 있습니다. 이 세계에서는 올바른 결정을 내릴 것이라는 신뢰에 의존할 필요가 없으며, 오히려 잘못된 행동을 할 수 없는 환경이 조성됩니다.

이것은 완전히 다른 세상입니다.

그리고 여러분도 이 세상을 만드는 데 동참할 수 있습니다. 비트코인을 사용하고 노드를 운영하며 주변 사람들에게 미래의 돈에 대해 더 많이 알리는 것만으로도 여러분은 새로운 세상을 선택하는 데 한 표를 행사하는 것입니다.

체험 활동: 수업 토론 – 여러분의 관점은 어떻게 변했는가?

아래 다섯 가지 질문을 답변해 주세요



제 10장

왜 우리는 돈이 필요한가?

돈이란 무엇인가?

왜 비트코인인가?

돈은 누가 통제하는가?

돈은 무엇 때문에 가치가 있는가?



제 10장

1장에서 선택한 질문과 답변을 작성하세요

1

1장의 첫 번째 체험 활동에 작성한 답변과 이번에 새로 작성한 답변을 비교합니다.

2

기존 답변과 질문을 논의해 보세요. 무엇이 달라졌나요?

3

그리고 스스로에게 질문을 합니다: “나의 다음 단계는 무엇인가?” “이 새로운 지식을 활용하여 나 자신을 성장시킬 수 있을까?”



다음 단계로 나아갈 준비가 되었다면, 다음 페이지에서 제공하는 추가 자료를 확인해 보세요.

더 깊이 있는 학습을 위해 최적의 자료들을 선별해 두었습니다.

추가 자료

1. 비트코인은 무엇일까?

“아토믹 비트코인” (X: @atomicBTC)

비트코인 기초부터 심화까지, 과정별로 안내하는 비트코인 소개와 기술 그리고 보고서 분석자료로 모든이에게 적합합니다.

“1분 비트코인” (유튜브: @1min_bitcoin)

비트코인을 처음 배우는 사람에게 도움이 되는 쉬운 설명과 상황극으로 비트코인을 안내합니다.

“네덜란드 땀 바보” (유튜브: @네덜바)

비트코인 전용 교육 채널로, 비트코인과 관련된 셀프커스터디와 기존 명목화폐의 문제점을 알려줍니다.

“비트코인 지식저장소” (유튜브: orangepillkr)

비트코인 뉴스부터 기술 내용까지 상세하게 번역된 음성으로 알려줍니다.

2. 비트코인 참여 과정

Bitcoin Social Layer (국내: <http://BSL.pub>)

한국에서 비트코인을 더 가치 있고 지속 가능한 사회를 만들어가는 그룹으로, 비트코인 입문 교육부터 비트코인 자격증, 채굴기 조립, 비트코인 결제매장 보급 등 참여과정 존재.

Summer of Bitcoin (해외, <https://www.summerofbitcoin.org>)

대학생들에게 비트코인 오픈소스 개발 및 디자인을 소개하는 글로벌 온라인 여름 인턴십 프로그램.

Chaincode Labs (해외, <https://learning.chaincode.com/#FOSS>)

온라인 과정 및 거주형 프로그램을 제공하여 학생들이 비트코인 프로토콜 개발에 필요한 기술을 학습할 수 있도록 지원.

Saylor Academy (해외, <https://www.saylor.org>)

여러 학문 분야에서 무료 교육을 제공하는 온라인 아카데미.

3. 기타 참고자료

Bitcoin.org: 비트코인 프로토콜 공식 웹사이트.

NOSTR: 탈중앙화 소셜미디어 서비스.

Bitcoinwiki.org: 비트코인과 관련된 모든 것을 포괄적으로 안내하는 비트코인 백과사전.

Mempool.Space: 오픈 소스 Mempool 프로젝트로, 비트코인 주소, 거래ID 등 모든 것을 조회하는 사이트.

Bitcoin-Design: 일러스트레이션, 웹사이트, 템플릿, 아이콘 등을 위한 오픈 소스 저장소인 비트코인 관련 디자인 파일.

bitrefill.com: 비트코인으로 상품권, 호텔, 비행기 티켓까지 모든 것을 구매할 수 있는 사이트.



1장:



과정 소개:

비트코인 디플로마 과정의 목표와 기대 사항을 탐색.



되돌아보기 - 돈 정의하기:

돈에 대한 핵심 질문에 대해 다섯 가지 답변을 제공하며 성찰하는 활동에 참여.



수업 토론 - 왜 돈이 필요한가?:

- ◆ 돈이 왜 필요한지에 대해 전체 수업 토론에 참여.
- ◆ 돈의 중요성에 대한 여러분 관점을 공유하고 비교.
- ◆ 경제 시스템에서 돈의 역할을 이해하는 기초 다지기.

2장:



돈을 이해하기:

- ◆ 돈의 원래 정의와 개념을 탐색.
- ◆ 돈의 다양성을 이해하기 위해 여러 관점을 논의.



기능, 속성, 유형:

- ◆ 돈의 기능, 속성, 유형에 대해 깊이 탐구.
- ◆ 돈을 정의하고 활용하는 데 있어 이러한 요소들이 왜 중요한지 인식.



돈의 심리학:

- ◆ 돈의 희소성, 시간 선호, 선택의 갈등 등을 이해.
- ◆ 심리 요소를 실제와 연결하는 시간 선호 활동에 참여.

3장:



돈의 역사와 발전 소개:

돈의 역사와 발전 과정을 탐색합니다. 고대의 교환 방식이 오늘날 화폐 발전에 기여한 요인을 이해.



화폐의 진화:

조개껍데기, 구슬과 같은 고대 화폐가 주화와 지폐로 변화하는 과정을 탐색. 종이 화폐에서 플라스틱(카드)까지의 발전을 통해 화폐의 역사를 이해.



디지털 화폐 혁명:

- ◆ 돈의 가장 현대 화폐인 디지털 화폐를 탐구합니다.
- ◆ 디지털 화폐가 전자로만 존재하며, 빠르고 저렴한 글로벌 거래가 가능하다는 점을 이해.
- ◆ 비트코인이 초기 디지털 화폐의 문제를 해결하고 글로벌 거래를 위해 준비되어온 과정을 학습.



물물교환 게임:

직접 교환 방식의 어려움을 체험하는 게임 활동에 참여. 보다 효율적인 화폐 시스템의 필요성을 인식.

핵심 개념

4장:

명목화폐의 기원:

명목화폐의 기원을 간략한 역사를 통해 탐색하고, 주요 화폐 형태가 된 이유를 이해.

부분준비금 제도 활동:

부분준비금 제도를 체험하는 활동에 참여하여 이 시스템이 작동하는 방법을 이해하고, 부채에 대한 의존성과 경제 전반에 미치는 영향을 분석.

명목화폐 시스템:

명목화폐 시스템의 기본 개념을 이해하고, 정부가 법령으로 정하는 화폐 제도의 특성, 부분준비금 은행제도의 역할, 이 시스템을 관리하는 주요 기관에 대해 학습.

5장:

구매력 감소:

통화 인플레이션 개념과 구매력에 미치는 영향을 이해. 인플레이션 효과: 경매에 참여하여 그 영향을 직접 경험.

명목화폐 시스템의 결과 활동:

명목화폐 시스템이 초래하는 광범위한 경제적 영향을 탐구하는 활동에 참여함.

중앙은행 디지털화폐(CBDC):

중앙은행 디지털화폐(CBDC) 발전 현황과 미래 화폐 시스템에 미칠 영향을 탐색.

세계 부채 부담과 사회 불평등:

세계 부채 부담과 사회 불평등이 미치는 이중적인 영향을 탐구함. 구매력 감소 및 부의 격차 확대 등 개인과 사회에 미치는 영향을 인식.

사이퍼펑크(Cypherpunks)와 탈중앙화:

사이퍼펑크 운동의 역사와 탈중앙화 화폐를 추구하는 동기를 학습. 중앙화 시스템과 탈중앙화 시스템의 차이를 이해하고, 디지털 화폐의 역사를 학습.

6장:

사토시 나카모토와 비트코인의 탄생:

비트코인 창시자인 사토시 나카모토와 비트코인의 기원에 대해 탐구하며 비트코인 개발 동기를 이해.

수업 활동 - 합의 형성:

P2P 네트워크 내에서 합의가 이루어지는 방법을 실습하는 활동에 참여.

개인 책임 강조:

비트코인 생태계에서 책임과 역할을 강조. 탈중앙화에서 책임감 있는 행동과 윤리 원칙을 이해하도록 장려.

비트코인의 작동 원리:

비트코인의 기술 작동 방식을 탐구. 나카모토 합의 메커니즘, 비트코인 네트워크 주요 참여자(채굴자, 노드, 사용자, 개발자, 프로젝트) 등 협력을 이해.

건전한 디지털 화폐로서 비트코인:

비트코인의 진화, 기능, 특성을 논의하고, 비트코인이 건전한 화폐인지에 대한 수업 토론에 참여함.

7장:

P2P(개인 간) 거래:

거래를 직접 경험하며 비트코인 거래의 핵심 원칙을 탐색.

비트코인 지갑 설정:

비트코인 지갑을 다운로드하고, 키를 생성하며, 보안 거래를 위한 백업 방법을 학습.

저축과 DYOR:

비트코인을 가치 저장 수단으로 이해하고, DYOR(Do Your Own Research) 중요성을 배움.

비트코인 지갑 유형:

오픈 소스, 클로즈드 소스, 커스터디얼(관리형), 논커스터디얼(비관리형) 지갑 차이를 이해하고, 보안에서 키 역할을 학습.

비트코인 획득:

P2P 거래 및 거래소를 통한 비트코인 획득 방법을 탐색하고, KYC(Know Your Customer) 프로세스와 관련된 개인정보 보호 문제를 논의.

8장:

라이트닝 네트워크 소개:

비트코인 확장성을 향상시키는 라이트닝 네트워크 기술 발전과 기능을 탐구.

라이트닝 지갑 설정:

비트코인 라이트닝 지갑을 설정하는 필수 단계를 배우고, 더 빠르고 확장 가능한 거래를 수행하는 방법을 익힘.

실습 활동:

라이트닝 네트워크 지갑 릴레이 경주에 참여하여, 라이트닝 거래를 실습하고 이해를 심화.

라이트닝 지갑 유형:

오픈 소스, 비공개 소스, 셀프커스터디, 수탁형 라이트닝 지갑의 차이를 비교하고, 사용자 선호도에 따라 선택하는 방법을 학습.

라이트닝 거래:

라이트닝 네트워크를 통한 송금 및 수금 과정을 탐색하고, 속도와 효율성을 강조.

9장:

비트코인 원장:

비트코인 네트워크에서 노드와 채굴자가 유지하는 탈중앙화 개념을 이해하고, 보안의 역할을 학습.

UTXO 모델:

비트코인 거래 처리에서 중요한 미사용 거래 출력(UTXO, Unspent Transaction Output) 모델을 탐색.

공개키와 개인키:

비트코인 거래에서 암호화가 중요한 이유를 학습하고, 공개키와 개인키 역할을 이해. SHA-256 해싱 알고리즘을 시연하는 활동을 수행.

비트코인 노드와 채굴자:

비트코인 네트워크에서 노드와 채굴자가 수행하는 역할을 학습하고, 발행(issuance), 희소성(scarcity), 반감기(halving), 채굴 난이도(difficulty) 등을 탐구.

비트코인 거래 작동 방식:

비트코인 거래의 전체 과정(보내는 사람, 받는 사람, 노드, 채굴자, 멤풀 포함)을 이해하고, 메모리풀 역할에 초점을 맞춘 학습을 진행.

핵심 개념

10장:



비트코인의 철학:

비트코인의 철학을 탐구하고, 명목화폐 시스템의 경제 위기에 대한 해답으로 이해. 금융 주권에 미치는 영향과 기존 화폐와 차이점을 중점적으로 학습함.



비트코인의 미래:

비트코인의 향후 발전 가능성과 미래 전망을 혁신있는 디지털 화폐 관점에서 탐구.



디플로마 되돌아보기:

비트코인 디플로마 과정에서 얻은 핵심 내용을 정리하며 각자 학습한 내용을 되돌아보며 왜 비트코인인가? 영상 시청. 1장 질문을 다시 확인하여 생각이 바뀌었는지 확인.



51% 공격 (51% Attack): 타임체인 네트워크에서 단일 주체 또는 그룹이 네트워크 컴퓨팅 파워(해시율) 과반수를 장악하여 거래 조작을 하는 공격.

알트코인 시즌 (Altcoin Season): 비트코인을 제외한 암호화폐 가격이 급등하는 기간으로, 일반적으로 투기 때문에 발생.

알트코인 (Altcoins): 비트코인을 제외한 모든 코인.

아토믹 스왑 (Atomic Swap): 중앙화 거래소나 중개자 없이, 암호화폐 간 P2P(개인 간) 교환을 가능하게 하는 기술.

경매 (Auction): 상품이나 자산을 최고 입찰자에게 판매하는 과정.

물물교환 (Bartering): 돈을 사용하지 않고 상품과 서비스를 직접 교환하는 방식.

상품 바스켓 (Basket of Goods): 생활비 변화를 측정하기 위해 사용되는 상품 및 서비스 모음.

비트코인 (Bitcoin): 은행 없이 사람들끼리 직접 송금이 가능한 디지털 화폐 및 시스템.

블록 탐색기 (Block Explorer): 타임체인 상의 개별 블록, 거래 내역, 지갑 주소 등을 조회할 수 있는 도구.

블록 보상 (Block Reward): 새로운 블록을 타임체인에 추가한 채굴자에게 지급되는 새로 발행되는 비트코인.

비티씨 (BTC): 비트코인의 단위. 구매 또는 거래에 사용할 수 있는 디지털 화폐.

자본 통제 (Capital Controls): 자금의 국경 간 이동을 제한하는 정책.

중앙은행 (Central Bank, Fed): 국가 통화 정책을 관리하는 정부 소유 기관.

중앙화 (Centralization): 권력 또는 통제 권한이 단일 기관에 집중된 상태.

중앙화 시스템 (Centralized System): 단일 기관이 권한을 가지는 구조.

콜드 스토리지 (Cold Storage): 비트코인을 해커나 온라인 위협으로부터 보호하기 위해 오프라인에서 보관하는 방식.

상품 화폐 (Commodity Money): 가치가 있는 물건을 교환 매개체로 사용하는 화폐(예: 금, 은).

확인 (Confirmation): 거래가 네트워크에 의해 처리되어 되돌릴 가능성이 매우 낮아지는 과정. 채굴자들이 컴퓨터 하드웨어와 소프트웨어를 사용하여 거래 진위성을 확인하는 방법이며 이중 지불을 방지하려면 최소 6번 확인을 기다리는 것이 권장됩니다.

합의 메커니즘 (Consensus Mechanism): 거래를 검증하고 타임체인 무결성을 보장하는 데 사용되는 방법.

암호화폐 거래소 (Cryptocurrency Exchange): 사용자가 명목화폐나 다른 암호화폐를 사고팔고 거래할 수 있는 플랫폼.

암호화폐 지갑 (Cryptocurrency Wallet): 개인키를 저장하고 사용자가 암호화폐를 보내고, 받고, 관리할 수 있게 하는 소프트웨어 프로그램.

용어집

암호학 (Cryptography): 안전한 시스템을 만드는 데 도움이 되는 수학의 한 분야.

화폐 가치 하락 (Debasement): 화폐 가치가 줄어드는 것, 주로 주화에서 귀금속의 양을 줄임으로써 발생.

부채 (Debt): 다른 사람에게 빚진 돈.

탈중앙화 (Decentralization): 권한과 통제가 네트워크 전반에 분산되는 것.

탈중앙화 시스템 (Decentralized System): 권한이나 통제가 여러곳에 분산된 시스템.

디지털 자산 (Digital Asset): 비트코인과 같은 가치의 디지털 표현으로, 거래되거나 가치 저장 수단으로 사용될 수 있는 것.

디지털 장부 (Digital Ledger): 한 곳에 저장되지 않고 컴퓨터 네트워크에 걸쳐 분산된 데이터베이스.

이중 지불 (Double Spending): 비트코인을 동시에 두 명의 수령자에게 자신의 비트코인을 보내는 것을 시도하는 것.

먼지 거래(공격) (Dust Transaction): 거래 수수료보다 작은 비트코인 거래를 뜻하며, 비트코인 주소 개인키 소유주의 신원을 찾기 위한 하나의 공격 방법.

환율 (Exchange Rate): 한 통화가 다른 통화와 관계에서 가지는 가치.

포모 (FOMO): 놓칠까 봐 두려움(Fear of Missing Out), 수익 기회를 놓칠지도 모른다는 불안을 뜻하는 용어.

퍼드 (FUD): 두려움, 불확실성, 의심(Fear, Uncertainty, Doubt), 시장 하락을 유발할 수 있는 근거 없지만 부정적인 소문이나 정보를 묘사하는 용어.

국내총생산 (GDP): 일정 기간 동안 한 국가에서 생산된 상품과 서비스의 총 가치를 의미하는 국내총생산.

하드 포크 (Hard Fork): 새로운 비트코인 프로토콜이 이전 버전과 호환되지 않는 것.

하드웨어 지갑 (Hardware Wallet): 개인키를 저장하고 관리하는 데 사용되는 물리 장치. 개인키를 저장하지 않는 물리 장치도 존재.

해시 함수 (Hash Function): 임의 크기의 입력 데이터를 받아 고정된 크기의 문자열(해시)로 출력하는 수학적 함수.

해시율 (Hash Rate): 비트코인 네트워크의 처리 능력을 측정하는 방법.

호들 (HODL): 비트코인을 장기 보유하자는 HOLD의 오타로 시작되었지만, 밍이 된 용어.

핫 월렛 (Hot Wallet): 인터넷에 연결된 비트코인 지갑으로, 콜드 월렛을 사용하는 것을 권장..

수입 (Imports): 다른 국가에서 생산되어 국내 시장에서 판매되는 상품과 서비스.

인플레이션 (Inflation): 경제 내에서 상품과 서비스 가격이 상승하는 것.



초기 코인 판매 (Initial Coin Offering, ICO): 새로운 암호화폐를 미리 투자자에게 판매하는 자금 조달 방법.

레이어-1 프로토콜 (Layer-1 Protocol): 타임체인의 기본 레이어로, 합의, 거래 검증, 데이터 저장과 같은 것을 처리.

레이어-2 프로토콜 (Layer-2 Protocol): 레이어-1 네트워크 위에 구축된 두 번째 레이어로, 확장성, 속도, 기능성을 향상시키는 데 사용.

장부 (Ledger): 금융 거래 기록.

라이트닝 네트워크 (Lightning Network): 더 빠르고 저렴한 비트코인 거래가 가능한 레이어-2 결제 프로토콜로, 소규모 거래를 위해 오프체인 채널을 활용.

교환 매개체 (Mediums of Exchange): 상품과 서비스 교환에 사용되는 물건이나 시스템.

머클 트리 (Merkle Tree): 비트코인 타임체인에서 데이터를 효율적으로 검증하기 위해 사용되는 트리 형태의 데이터 구조.

채굴 풀 (Mining Pool): 새로운 블록을 찾아 비트코인을 얻을 확률을 높이기 위해 함께 작업하는 채굴자 그룹.

채굴 (Mining): 비트코인 네트워크에서 거래를 확인하고 보안을 강화하기 위해 컴퓨터 하드웨어를 사용하여 수학적 계산을 수행하는 과정.

통화 및 재정 정책 (Monetary and Fiscal Policy): 중앙은행과 정부가 각각 경제 내 통화 공급과 재정 정책에 미치는 영향.

통화 공급 (Money Supply): 경제 내에서 유통되는 총 통화량.

멀티시그 지갑 (Multi-Signature(Multisig) Wallet): 거래를 서명하기 위한 키가 여러 개로 구성된 지갑으로, 추가적인 보안과 통제력을 제공합니다.

네트워크 (Network): 상호 연결된 개체들의 그룹.

노드 네트워크 (Node Network): 비트코인 네트워크를 지원하고 유지하는 연결된 컴퓨터 또는 네트워크.

노드 (Node): 비트코인 네트워크에 연결되어 거래 검증과 전송에 참여하는 컴퓨터 또는 장치.

논스 (Nonce): 목표 난이도를 총족하는 해시를 생성하기 위해 블록 헤더에 추가되는 임의의 숫자.

페이퍼 지갑 (Paper Wallet): 비트코인을 저장하고 관리하기 위해 사용자 개인키와 공개키를 인쇄한 종이 사본.

개인 대 개인 (Peer-to-Peer, P2P): 참여자들이 거래소를 통하지 않고 직접 거래하는 탈중앙화 네트워크.

페그 (Peg): 두 통화 간 고정된 환율로, 한 통화의 가치가 다른 통화에 고정.

개인키 (Private Key): 특정 지갑에서 비트코인을 사용할 권한을 증명하는 비밀 데이터로, 암호화 서명을 통해 사용됨.

작업 증명 (Proof-of-Work): 네트워크에 참여하기 위해 사용자가 컴퓨터 계산 작업을 수행해야 하는 합의 메커니즘.

용어집

공개키 (Public Key): 사용자 개인키에서 수학적 과정을 통해 파생된 비트코인을 받는 데 사용되는 고유 식별자.

공개키/비트코인 주소 (Public Key/Bitcoin Address): 비트코인을 받는 데 사용되는 공개 비밀번호/숫자.

공개 장부 (Public Ledger): 비트코인 네트워크에서 모든 거래를 공개적으로 기록하는 탈중앙화 데이터베이스.

구매력 (Purchasing Power): 돈으로 상품과 서비스를 구매할 수 있는 능력.

복구 구문/시드 키워드 (Recovery Phrase/Seed Keyword): 비트코인 지갑을 복원하는 데 사용할 수 있는 12개, 18개 또는 24개 단어로 구성된 단어 조합으로, 여러 쌍의 개인키와 공개키를 생성하는 데 사용.

지금준비율 (Reserve Ratio): 은행이 예금 중 보유해야 하는 준비금의 비율.

은행업 규제 (Restrictive Banking): 자금세탁방지, 고객알기제도, 금산분리 등 은행 내외 제도나 규제.

사토시 나카모토 (Satoshi Nakamoto): 비트코인의 익명 창시자가 사용한 가명.

사토시 (Satoshi): 비트코인의 최소 단위로, 1비트코인 1억분의 1($1/100,000,000$)이며, 비트코인 창시자인 사토시 나카모토의 이름을 따서 명명됨.

바이트당 사토시 (Satoshi per Byte, sat/b): 거래 데이터의 바이트당 지불되는 비트코인 거래 수수료를 측정하는 단위.

세그윗 (SegWit, Segregated Witness): 비트코인 프로토콜 업그레이드로, 타임체인에 데이터 저장 방식을 변경하여 용량을 늘리고 거래 수수료를 낮춤.

사이드체인 (Sidechain): 다른 블록체인에 연결된 타임체인으로, 두 체인 간 자산 또는 정보 이전을 허용.

서명 (Signature): 소유권을 증명하는 수학적 메커니즘.

소프트 포크 (Soft Fork): 비트코인 프로토콜에 기존 버전과 호환되는 소프트웨어를 적용하는 것.

스테이블코인 (Stablecoin): 명목화폐나 기타 국채에 고정되어 안정적인 가치를 유지하도록 설계된 암호화폐.

스테일 블록 (Stale Block): 더 긴 경쟁 체인에 의해 무효화되어 타임체인에 포함되지 않은 블록.

공급과 수요 (Supply and Demand): 상품이나 서비스 가격이 공급과 수요 상호로 결정되는 경제 원리.

타임체인 (Timechain): 모든 비트코인 거래 내역이 기록된 공개 장부(분산 원장).

돈의 시간 가치 (Time Value of Money): 돈이 현재보다 미래에 더 가치가 있다는 원리.

거래 쌍 (Trading Pair): 거래소에서 서로 교환 가능한 두 통화.

거래 수수료 (Transaction Fee): 비트코인을 보내는 사람이 채굴자에게 지불하는 소량의 비트코인으로, 거래를 블록에 포함하고 타임체인에 추가하도록 유도.



거래 ID (Transaction ID): 비트코인 전송 세부사항(보낸 금액, 주소, 전송 날짜 등)을 보여주는 숫자와 문자열.

거래 (Transaction): 비트코인 네트워크에서 한 주소에서 다른 주소로 비트코인을 전송하는 것.

무 신뢰성 (Trustless): 제3자나 중개자에 대한 신뢰가 필요 없는 시스템 또는 거래로, 기저 기술의 보안성과 투명성에 의존.

2단계 인증 (Two-Factor Authentication, 2FA): 계정에 접근하거나 거래를 완료하기 위해 두 가지 인증 방법(일반적으로 비밀번호와 별도의 코드 또는 장치)이 필요한 보안 조치.

언뱅크드 (Unbanked): 은행 서비스에 접근하지 못하는 개인 또는 커뮤니티.

회계 단위 (Unit of Account): 상품과 서비스 가치를 표현하는 데 사용되는 표준 측정 단위.

변동성 (Volatility): 자산 가격이 시간에 따라 변동하는 정도.

지갑 주소 (Wallet Address): 비트코인 네트워크에서 비트코인을 보내고 받는 데 사용되는 고유 식별자로, 보통 문자와 숫자 나열로 표현.

지갑 백업 (Wallet Backup): 비트코인 지갑의 개인키와 복구 구문/시드 키워드의 복사본으로, 원본이 분실되거나 도난당했을 경우 지갑에 다시 접근하는 데 사용.

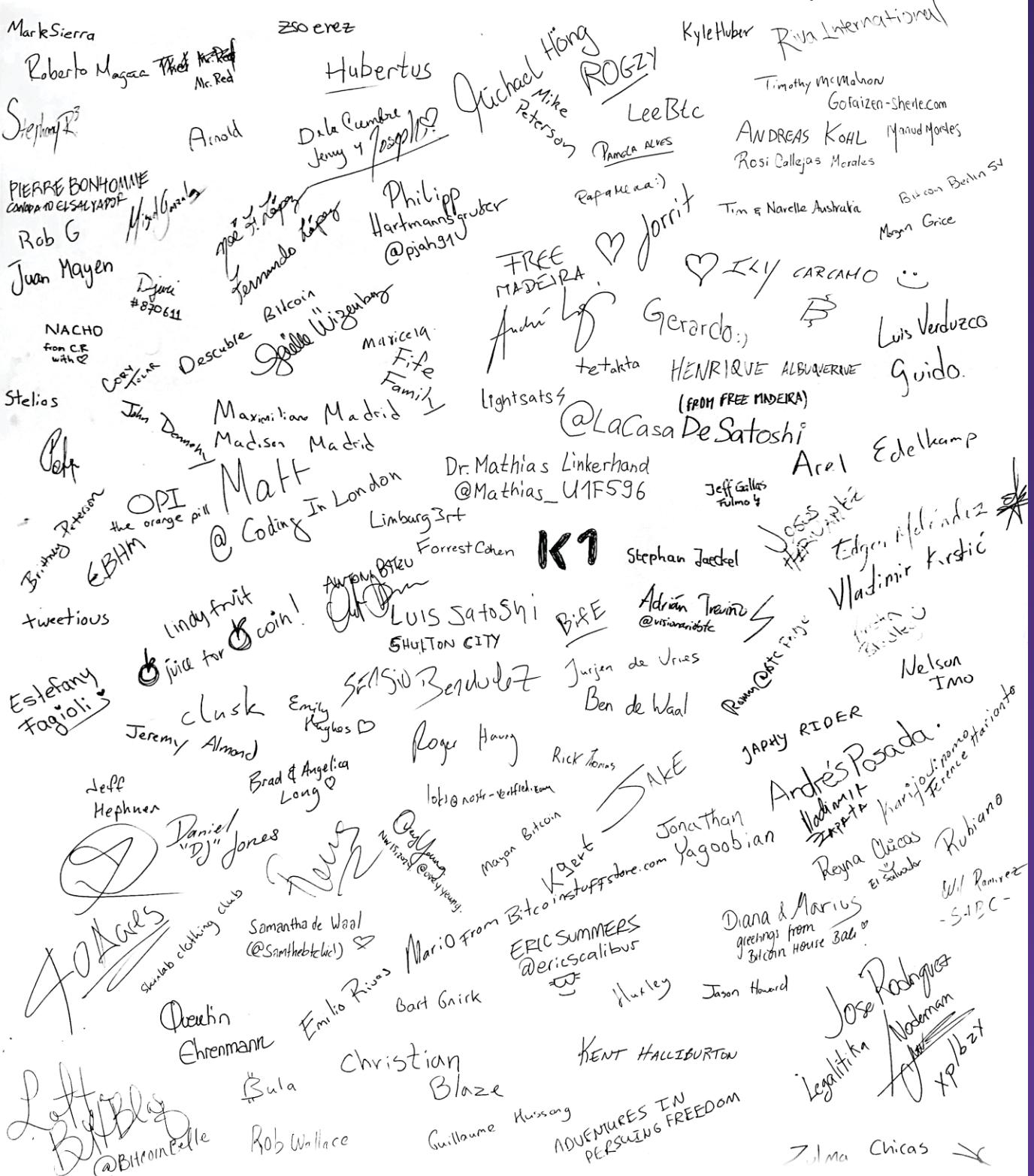
지갑 (Wallet): 비트코인을 저장하는 가상 컨테이너로, 비트코인을 사용할 수 있는 개인키를 포함하며 물리 지갑과 유사.

화이트 햇 해커 (White Hat Hacker): 시스템과 네트워크의 취약점을 찾아내고 해결하는 데 기술을 사용하는 윤리적인 해커.

용어집

여러분 덕분에 독립했습니다

2024년 Geyser 캠페인 또는
Adopting Bitcoin에 기부해 주신
기부자 여러분께 감사드립니다.



고마워요!



한국어 버전 | 2025

